+

Remote Administrative Software (RAS)

By

GC UMAR QAYYUM MINHAS

PC FAISAL JAVED BAJWA

PC AQSAM LIAQAT CHEEMA

Supervised by:

LT COL USMAN MEHMOOD MALIK

Submitted to the faculty of Department of Computer Software Engineering,
Military College of Signals, National University of Sciences and Technology, Islamabad,
in partial fulfillment for the requirements of B.E Degree in Software Engineering.
June 2023

“In the name of ALLAH, the Most compassionate,the Most merciful”

CERTIFICATE OF CORRECTNESS AND APPROVAL

This is to officially state that the thesis works in this report

“Remote Administrative Software”

is carried out by

GC UMAR QAYYUM MINHAS
PC FAISAL JAVED BAJWA
PC AQSAM LIAQAT CHEEMA

under my supervision and according to my judgement, it fully ample, in scope and excellence, for degree of Bachelor of Software Engineering in Military College of Signals, National University of Sciences and Technology (NUST), Islamabad.

Approved by
Supervisor
Lt Col Usman Mehmood

Date: ___________

DECLARATION OF ORIGINALITY

We solemnly hereby declare that no portion of work presented in this thesis report has been submitted in support of award or qualification in either this institute or anywhere else other than this.

ACKNOWLEDGEMENTS

Allah Subhan’Wa’Tala is the sole guidance in all domains.

Our Parents, Colleagues, Instructors and most of all our supervisor Lt Col Usman Mehmood Malik. Without your guidance and support it would have never been possible for us to complete our Final Year Project.

ABSTRACT

RAS is a sophisticated malleable and modern C2 framework designed for use by penetration testers, red teams, and blue teams. Its intuitive GUI and comprehensive feature set provide users with the ability to establish control, monitor activity, and perform post-exploitation actions. The platform's user interface is sleek and user-friendly, with additional features not commonly found in similar frameworks.

The Havoc Framework consists of two main components: the Teamserver, which manages connected operators, agents, and data, and the client, which provides users with an interface to interact with agents and receive output from them. The Teamserver should be hosted on a public VPS to allow registered operators access to the system.

RAS is designed to be a stealthy tool for ongoing data collection, following the principles of an advanced persistent threat (APT). Its power lies in its ability to remain undetected over long periods.

<Plagiarism Certificate>

<Turnitin Report>

Turnitin report endorsed by Supervisor is attached. This thesis has 8 % similarity index.

GC UMAR QAYYUM
00000325019

PC FAISAL JAVED
00000325371

PC AQSAM LIAQAT
00000325388

Signature of Supervisor
(LT COL USMAN MALIK)

Table of Contents

Chapter 1: Introduction

The introductory section of this document furnishes a comprehensive overview of the Final Year Project, encompassing its purpose, scope, definitions, acronyms, abbreviations, references, and a synopsis of the Software Design Document. The primary objective of this document is to present an intricate exposition of the project, namely the Remotely Administrative Software, which is intended to facilitate the management of an output device. This document expounds upon the elaborate structural design of the RAS in great detail.

An advanced persistent threat (APT) denotes the surreptitious and prolonged invasion of computer systems with the primary aim of accumulating data, without causing harm to the information or systems. In this type of attack, RAS serves as a potent instrument due to its ability to operate covertly without compromising a computer's performance, and its high degree of adaptability. Remote Access Trojans, unlike other forms of computer viruses such as keyloggers or ransomware, do not solely record data input or hold files hostage but rather provide hackers with complete administrative control over the infected system, as long as they evade detection.

1.1 Overview

Remote administration refers to the practice of remotely controlling one or multiple computers through an Internet connection, TCP / IP , or Local Area Network (LAN)s. This technique can serve various purposes, including managing multiple servers. The Remote Administration Tool (RAT) is a common tool employed for remote administration, which can be surreptitiously implanted to gain access to victim machines. Attackers can use various methods to inject RATs, such as through patches, updates, games, email attachments, or even in seemingly legitimate binaries.

To circumvent antivirus software installed on the victim's computer, RATs can be made fully undetectable we . Once installed, RATs can grant the attacker access to numerous directories, webcams, and keyboards. Additionally, keyloggers can be used to monitor and record the victim's keystrokes, and the attacker can take over the keyboard, rendering the victim unable to use it. RATs can also be employed to install other malicious programs, which can be injected via external storage devices such as pen drives or hard drives. These devices, commonly known as "bash bunnies," can install RATs, backdoors, and payloads merely by inserting the drive into the victim's computer.

RATs utilize processes to conceal their activities and inject running tasks with malicious code that evades detection by the system. The potential harm that RATs can cause includes Distributive Denial of Service (DDoS) attacks, obtaining sensitive information, and recording the actions of the current session of the system, such as screen previews and keystrokes. RATs can also redirect traffic to other systems for obtaining specific services.

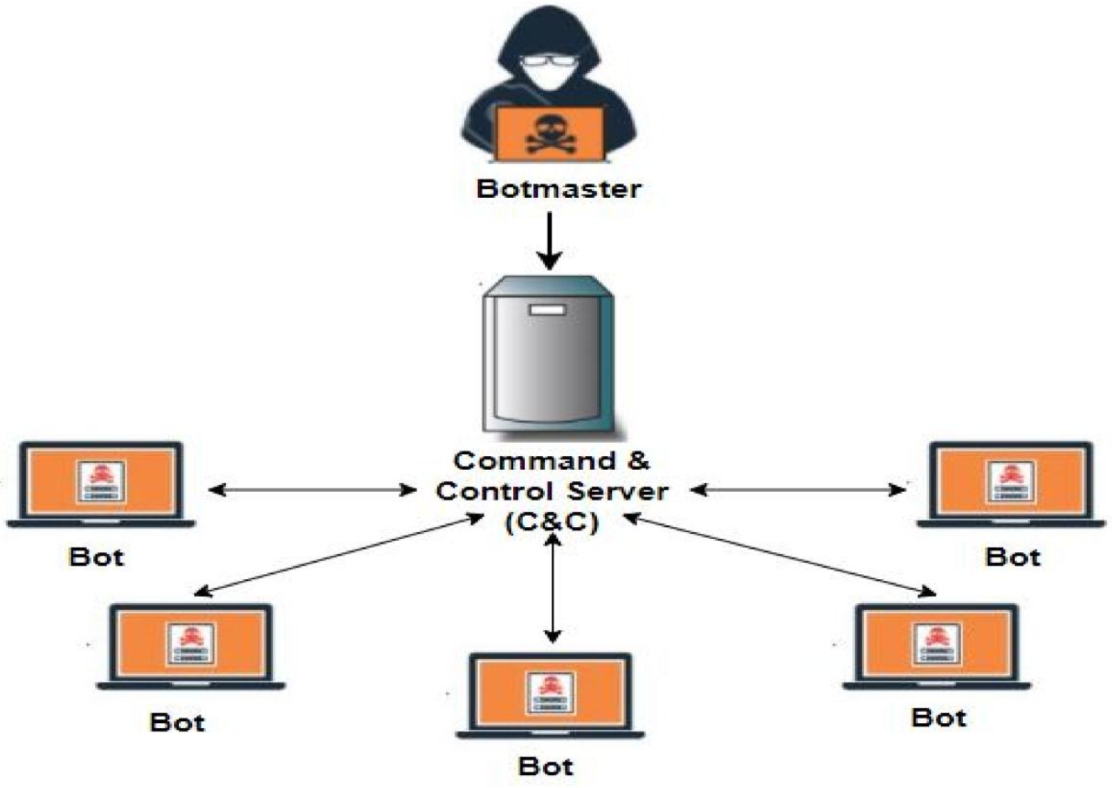
While intelligence agencies and law enforcement agencies can use RATs for monitoring and conducting surveillance on terrorists, anti-state agents, and pre-selected targets, it is critical to use these tools responsibly and within the bounds of the law. Any unauthorized usage of RATs can result in severe legal and ethical consequences.

1.2 Problem Statement

The rise and widespread use of modern communication and computing technology has caused a fundamental change in the way people conduct activities and communicate in contemporary society. Computers have become a ubiquitous tool and have transformed various aspects of life, such as online transactions, entertainment, gaming, education, and communication across multiple platforms. However, with the increasing accessibility of computers, they have also become a potential threat to law enforcement agencies who need to monitor and surveil potential threats, such as terrorists, anti-state agents, and other selected targets. Therefore, the use of computers for malicious purposes has become a significant concern in today's world.

1.3 Proposed Solution

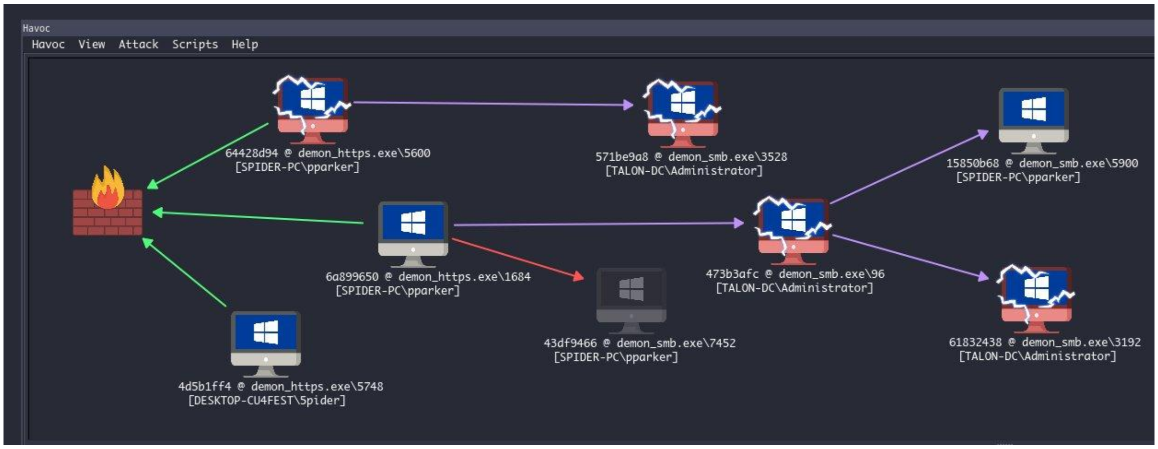
Considerable progress has been made on the Project to develop a Remote Administrative Software that can avoid detection. However, this demanding and time-consuming process makes it more appealing to hackers who target larger entities like governments, corporations, and financial institutions. The Remote Administrative Software can be utilized for surveillance and monitoring, making it a powerful tool for malevolent actors.



1.3 Working Principles

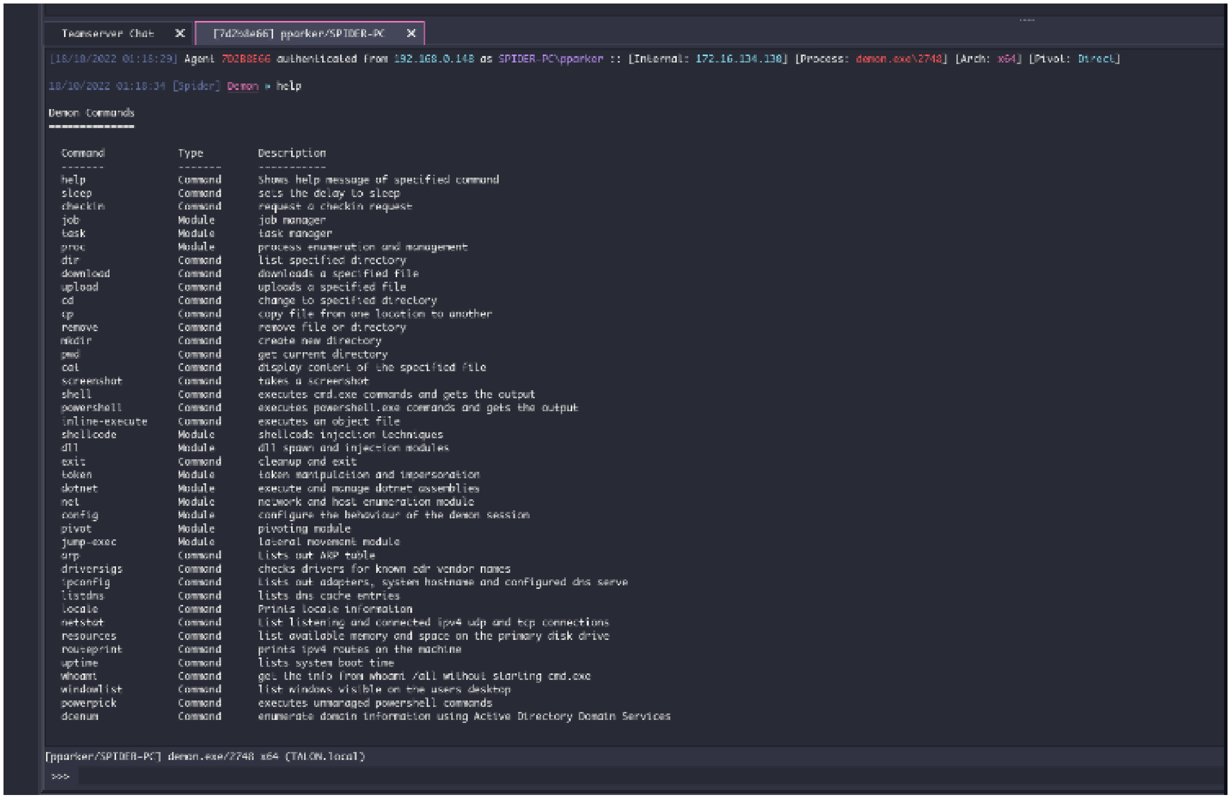
The Framework comprises two key components: the Teamserver and the Client. The former is responsible for managing connected operators, parsing callbacks and listeners, and handling tasks assigned to agents, including the collection of downloaded files and screenshots. For secure access, it is recommended that the Teamserver is hosted on a public virtual private server (VPS), which can only be accessed by authorized and registered operators. The Client, on the other hand, provides a user-friendly interface that allows users to easily interact with the system, assign tasks to agents, and retrieve output from them.

An abstract diagram for RAS is also provided below, which outlines how the system operates from module to module, intercepting and substituting system functions to render OS files invisible.


Havoc
Havoc View Attack Scripts Help
64428d94 @ demon_https.exe\5600
[SPIDER-PC\pparker]
571be9a8 @ demon_smb.exe\3528
[TALON-DC\Administrator]
15850b68 @ demon_smb.exe\5900
[SPIDER-PC\pparker]
6a899650 @ demon_https.exe\1684
[SPIDER-PC\pparker]
473b3afc @ demon_smb.exe\96
[TALON-DC\Administrator]
43df9466 @ demon_smb.exe\7452
[SPIDER-PC\pparker]
61832438 @ demon_smb.exe\3192
[TALON-DC\Administrator]
4d5b1ff4 @ demon_https.exe\5748
[DESKTOP-CU4FEST\5pider]

1.4.1 Input Component

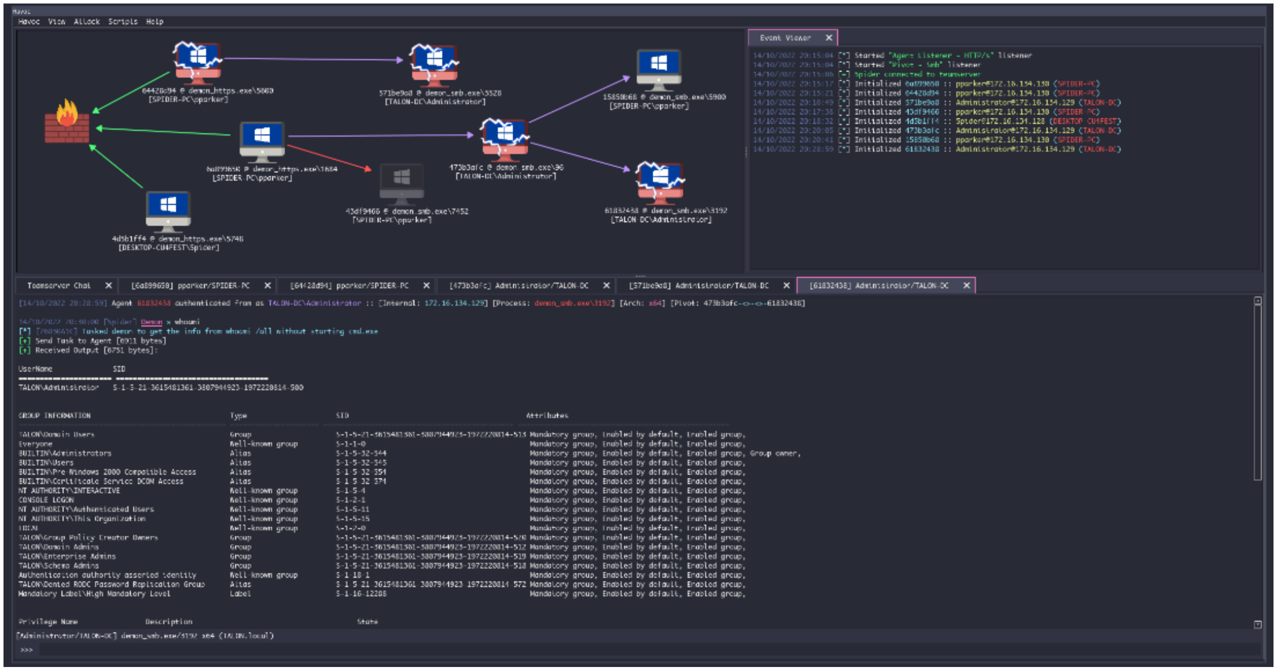
The RAS consists of two main components: the Teamserver and the Demon. The Teamserver, written in Golang, is responsible for generating payloads such as exe/shell code/dll, setting up HTTP/HTTPS listeners, and providing external and customizable C2 profiles. It acts as a control panel for creating and connecting to the RAS, and serves as the core server that manages listeners, communicates with agents, and executes operator commands. On the other hand, the Demon is the flagship agent of the RAS, written in C and ASM, with a range of built-in commands. The RAS Daemon uses sleep obfuscation and x64 return address spoofing to ensure its activities are concealed.



```
[18/10/2022 01:18:29] Agent 702B8E66 authenticated from 192.168.0.148 as SPIDER-PC\pparker :: [Internal: 172.16.134.130] [Process: demon.exe\2748] [Arch: x64] [Pivot: Direct]

18/10/2022 01:18:34 [Spider] Demon » help

Demon Commands
==============

  Command            Type         Description
  -------            -------      -----------
  help               Command      Shows help message of specified command
  sleep              Command      sets the delay to sleep
  checkin            Command      request a checkin request
  job                Module       job manager
  task               Module       task manager
  proc               Module       process enumeration and management
  dir                Command      list specified directory
  download           Command      downloads a specified file
  upload             Command      uploads a specified file
  cd                 Command      change to specified directory
  cp                 Command      copy file from one location to another
  remove             Command      remove file or directory
  mkdir              Command      create new directory
  pwd                Command      get current directory
  cat                Command      display content of the specified file
  screenshot         Command      takes a screenshot
  shell              Command      executes cmd.exe commands and gets the output
  powershell         Command      executes powershell.exe commands and gets the output
  inline-execute     Command      executes an object file
  shellcode          Module       shellcode injection techniques
  dll                Module       dll spawn and injection modules
  exit               Command      cleanup and exit
  token              Module       token manipulation and impersonation
  dotnet             Module       execute and manage dotnet assemblies
  net                Module       network and host enumeration module
  config             Module       configure the behaviour of the demon session
  pivot              Module       pivoting module
  jump-exec          Module       lateral movement module
  arp                Command      Lists out ARP table
  driversigs         Command      checks drivers for known edr vendor names
  ipconfig           Command      Lists out adapters, system hostname and configured dns serve
  listdns            Command      lists dns cache entries
  locale             Command      Prints locale information
  netstat            Command      List listening and connected ipv4 udp and tcp connections
  resources          Command      list available memory and space on the primary disk drive
  routeprint         Command      prints ipv4 routes on the machine
  uptime             Command      lists system boot time
  whoami             Command      get the info from whoami /all without starting cmd.exe
  windowlist         Command      list windows visible on the users desktop
  powerpick          Command      executes unmanaged powershell commands
  dcenum             Command      enumerate domain information using Active Directory Domain Services

[pparker/SPIDER-PC] demon.exe/2748 x64 (TALON.local)
>>>
```

1.4.2 Application Component

The RAS includes a client-side, cross-platform user interface that is written in C++ and Qt and features a modern, dark-themed interface based on Dracula. This interface allows administrators to remotely access and monitor target devices and perform operations on them. The interface is divided into three main sections.


Havoc
Havoc View Attack Scripts Help
64428d94 @ demon_https.exe\5060
[SPIDER-PC\pparker]
571be9a8 @ demon_smb.exe\3528
[TALON-DC\Administrator]
15858b68 @ demon_smb.exe\5900
[SPIDER-PC\pparker]
6a899658 @ demon_https.exe\1684
[SPIDER-PC\pparker]
473b3afc @ demon_smb.exe\96
[TALON-DC\Administrator]
43df9466 @ demon_smb.exe\7452
[SPIDER-PC\pparker]
61832438 @ demon_smb.exe\3192
[TALON-DC\Administrator]
4d5b1ff4 @ demon_https.exe\5748
[DESKTOP-CU4FEST\Spider]
Event Viewer
Teamserver Chat
[6a899658] pparker/SPIDER-PC
[64428d94] pparker/SPIDER-PC
[473b3afc] Administrator/TALON-DC
[571be9a8] Administrator/TALON-DC
[61832438] Administrator/TALON-DC

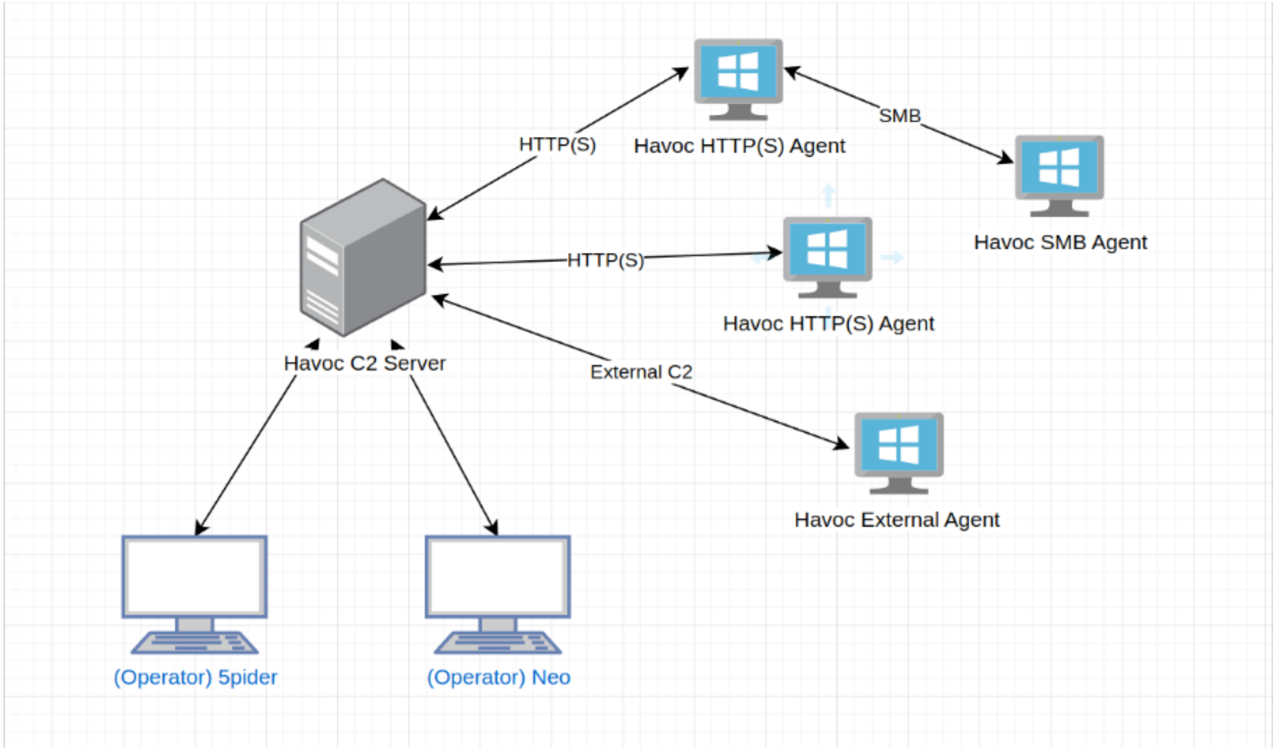
```
14/10/2022 20:15:04 [*] Started "Agent Listener - HTTP/s" listener
14/10/2022 20:15:04 [*] Started "Pivot - Smb" listener
14/10/2022 20:15:06 [-] Spider connected to teamserver
14/10/2022 20:15:17 [*] Initialized 6a899658 :: pparker@172.16.134.130 (SPIDER-PC)
14/10/2022 20:15:21 [*] Initialized 64428d94 :: pparker@172.16.134.130 (SPIDER-PC)
14/10/2022 20:16:49 [*] Initialized 571be9a8 :: Administrator@172.16.134.129 (TALON-DC)
14/10/2022 20:17:38 [*] Initialized 43df9466 :: pparker@172.16.134.130 (SPIDER-PC)
14/10/2022 20:18:32 [*] Initialized 4d5b1ff4 :: Spider@172.16.134.128 (DESKTOP-CU4FEST)
14/10/2022 20:20:05 [*] Initialized 473b3afc :: Administrator@172.16.134.129 (TALON-DC)
14/10/2022 20:20:41 [*] Initialized 15858b68 :: pparker@172.16.134.130 (SPIDER-PC)
14/10/2022 20:28:59 [*] Initialized 61832438 :: Administrator@172.16.134.129 (TALON-DC)
```

```
[14/10/2022 20:28:59] Agent 61832438 authenticated from as TALON-DC\Administrator :: [Internal: 172.16.134.129] [Process: demon_smb.exe\3192] [Arch: x64] [Pivot: 473b3afc-<>-<>-61832438]

14/10/2022 20:30:00 [Spider] Demon » whoami
[*] [70B9041C] Tasked demon to get the info from whoami /all without starting cmd.exe
[+] Send Task to Agent [6911 bytes]
[+] Received Output [6751 bytes]:

UserName              SID
====================  ===============================
TALON\Administrator   S-1-5-21-3615481361-3807944923-1972220814-500


GROUP INFORMATION                              Type              SID                                           Attributes

TALON\Domain Users                             Group             S-1-5-21-3615481361-3807944923-1972220814-513 Mandatory group, Enabled by default, Enabled group,
Everyone                                       Well-known group  S-1-1-0                                       Mandatory group, Enabled by default, Enabled group,
BUILTIN\Administrators                         Alias             S-1-5-32-544                                  Mandatory group, Enabled by default, Enabled group, Group owner,
BUILTIN\Users                                  Alias             S-1-5-32-545                                  Mandatory group, Enabled by default, Enabled group,
BUILTIN\Pre-Windows 2000 Compatible Access     Alias             S-1-5-32-554                                  Mandatory group, Enabled by default, Enabled group,
BUILTIN\Certificate Service DCOM Access        Alias             S-1-5-32-574                                  Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\INTERACTIVE                       Well-known group  S-1-5-4                                       Mandatory group, Enabled by default, Enabled group,
CONSOLE LOGON                                  Well-known group  S-1-2-1                                       Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\Authenticated Users               Well-known group  S-1-5-11                                      Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\This Organization                 Well-known group  S-1-5-15                                      Mandatory group, Enabled by default, Enabled group,
LOCAL                                          Well-known group  S-1-2-0                                       Mandatory group, Enabled by default, Enabled group,
TALON\Group Policy Creator Owners              Group             S-1-5-21-3615481361-3807944923-1972220814-520 Mandatory group, Enabled by default, Enabled group,
TALON\Domain Admins                            Group             S-1-5-21-3615481361-3807944923-1972220814-512 Mandatory group, Enabled by default, Enabled group,
TALON\Enterprise Admins                        Group             S-1-5-21-3615481361-3807944923-1972220814-519 Mandatory group, Enabled by default, Enabled group,
TALON\Schema Admins                            Group             S-1-5-21-3615481361-3807944923-1972220814-518 Mandatory group, Enabled by default, Enabled group,
Authentication authority asserted identity     Well-known group  S-1-18-1                                      Mandatory group, Enabled by default, Enabled group,
TALON\Denied RODC Password Replication Group   Alias             S-1-5-21-3615481361-3807944923-1972220814-572 Mandatory group, Enabled by default, Enabled group,
Mandatory Label\High Mandatory Level           Label             S-1-16-12288                                  Mandatory group, Enabled by default, Enabled group,


Privilege Name            Description                       State
[Administrator/TALON-DC] demon_smb.exe/3192 x64 (TALON.local)
>>>
```

1.4.3 Tools and Methodologies

Followings are the requirements to start the development process of the proposed system.

Amount different phases of RAS, Registration, Login, Payload Generation, HTTP/HTTPS Listening, C2 Profiles Customization will be done on the administrative side, whereas Target or client side will access payload to become vulnerable and give away access of the respective device to the Administrator over exploited network.



1.4..3 Hardware Requirements for setting up Development Environment

1. Dual Core Processors
2. 4 GB RAM
3. 40 GB Hard Disk

1.4.4 Software Requirements for Development Environment

1. Visual basic

2. Encrypter

3. Binder

4. Antivirus evasion tool

5. Different testing platforms

6. SSH Tunnels

5.1.5 Special Skills Required:

1. Encoding

2. Encryption

3. Social engineering

4. Binding

5. Bypassing/ Evasion of Antiviruses and different security tools

6. Crypting a code

7. Making software FUD

1.4.5 Languages

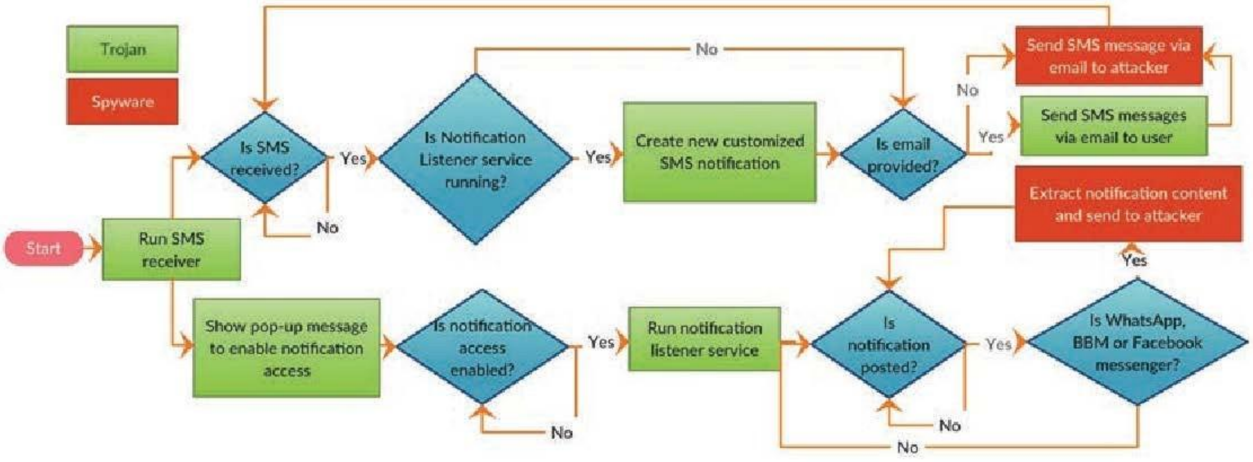
5 C++ and Qt

6 C and ASM

7 Golang

1.4.6 Output Component

The payload generated will be the output file which will be binded by any Legitimate attachment and will be crypted to evade the Antiviruses and firewalls.



Trojan
Spyware
No
Send SMS message via email to attacker
No
Send SMS messages via email to user
Yes
Is SMS received?
Yes
Is Notification Listener service running?
Yes
Create new customized SMS notification
Is email provided?
Extract notification content and send to attacker
No
Start
Run SMS receiver
Yes
Show pop-up message to enable notification access
Is notification access enabled?
Yes
Run notification listener service
Is notification posted?
Yes
Is WhatsApp, BBM or Facebook messenger?
No
No
No

Fig. 1: Application flowchart

1.5 Objectives

1.5.1 General Objectives:

The goal of RAS is to provide a contemporary adaptable and post-exploitation command and control architecture to implement the advanced persistent threat (APT), a method of continuing, covert hacking that seeks to gather data over time rather than harm information or systems. RAS is an effective weapon in this kind of assault since it is adaptive and won't cause a computer's performance to suffer or start destroying data on its own after installation.

1.5.2 Academic Objectives:

- Development of a smart and intelligent RAT system
- To implement Machine Learning techniques and simulate the results
- To increase productivity by working in a team
- To design a project that contributes to the welfare of society

1.6 Scope

The scope of RAS is to provide a malleable post-exploitation command and control C2 framework

- Exploiting network to capture data by intelligence agencies.
- To capture shared threats over the network by law forcing agencies,
- Intelligence agencies can use it to spy and capture data of enemies over the network.

1.7 Deliverables

Modern times have seen a significant increase in remote work and telecommuting, which has led to widespread usage of remote access solutions. These tools make it feasible for people to connect to computers and networks from distant locations, enabling them to work from home, communicate with team members who are in various places, and control systems remotely. However, using remote access tools has also sparked security worries because malicious actors and cybercriminals can use them to break into systems and steal confidential data. To reduce the dangers connected with the usage of remote access tools, it is crucial to install proper security measures and recommended practises.

1. Monitoring and surveillance of terrorist and anti-state agents
2. Security purposes
3. Intelligence purposes
4. Surveillance purposes
5. Data exploitation
6. Crime control

1.8 Relevant Sustainable Development Goals

Following are the relevant SDGs;

1 GOAL 9 - INDUSTRY, INNOVATIONS, AND INFRASTRUCTURE

2 GOAL 11 - SUSTAINABLE CITIES AND COMMUNITIES

3 GOAL 4 - QUALITY EDUCATION

4 GOAL 16 – JUSTICE,PEACE AND STRONG INSTITUTIONS

1.9 Structure of Thesis

Chap 2 contains literature review,background and analysis study of this thesis .

Chap 3 contains techniques

Chap 4 introduces the detailed data design.

Chap 5 introduces human interface design

Chap 6 comprises conclusion

Chap 7 highlights the work needed to be done in future for commercialization

Chapter 2: Literature Review

The main goal of this projects it to prepare software that can be used by law enforcing, intelligence for monitoring of purposes of terrorists, anti-state factors, and selected targets. It can also cover the needs for educational purposes.

2.1 Industrial background

Computing innovations have significantly impacted the way individuals interact in today's modern era of communication. Calls, texts, emails, sending and receiving instructions, online shopping, online banking, music streaming, and many more activities are all possible. One no longer has to carry along many gadgets because they can accomplish everything with only one. Today's ease of access has made it a real danger to LEAs when it comes to tracking down and monitoring terrorists, anti-state operatives, and pre-selected targets.

The scope of RAS is to provide a malleable post-exploitation command and control
C2 framework

- Exploiting network to capture data by intelligence agencies.
- To capture shared threats over the network by law forcing agencies,
- Intelligence agencies can use it to spy and capture data of enemies over the network.

2.2 Existing solutions and their drawbacks

Pakistan doesn’t have any indigenous technologies in such field to monitor the activities of suspicious factors. Due to easily access to computing technology now a days, it has emerged as a serious threat against law enfocing agencies in surveillance of terrorists, anti-state factors, and selected targets.

• The majority of viruses are connected to .exe files, so even if one is already on your computer, it wont be infecting it until unless you don’t execute them.

People assist the spread of computer virus, most of the times unknowingly.

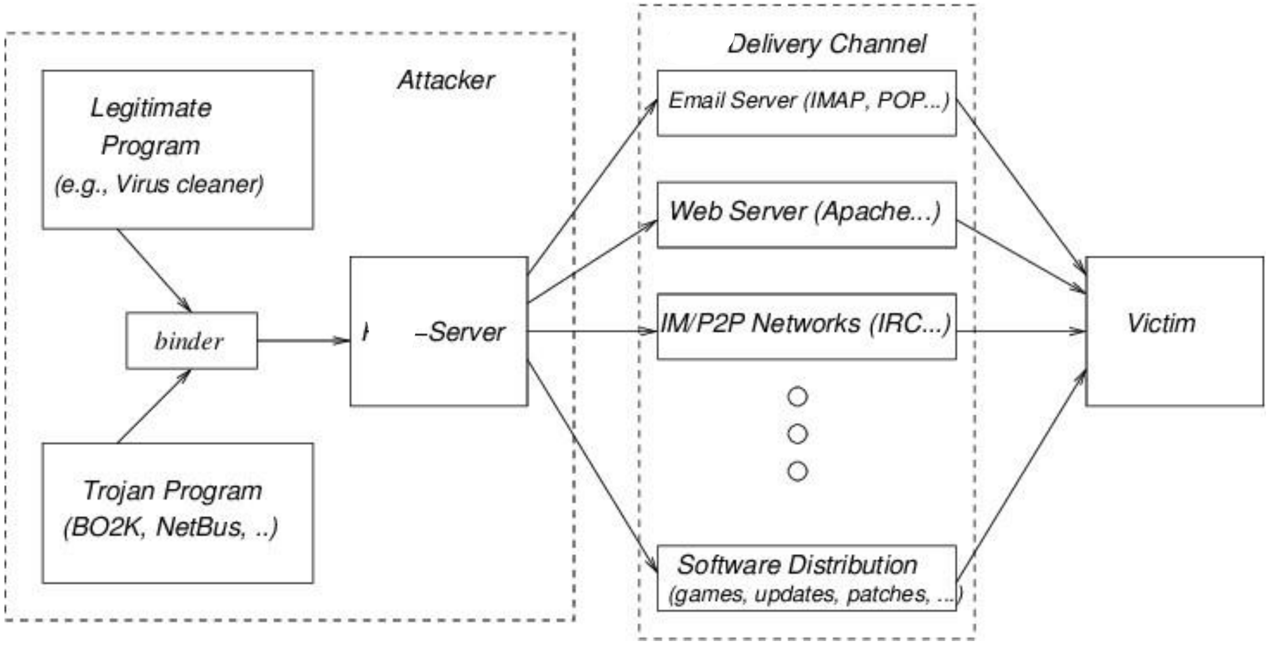
• For propagating one to another computer and infecting additional along side, a virus attaches itself to files or progarams.

- A keylogger records every typed keystroke determining usernames, passwords and credit card details, etc., and sensitive and personal information.
- RAS is inclusive of a back door for administrative powers over target.

Chapter 3: Techniques

3.1 Techniques

Remote Administrative Software is a tool that enables remote control of a computer, yet malicious actors can exploit it for nefarious purposes. They employ methods such as fraudulent links, torrents, and email attachments to install this software on a victim's computer surreptitiously. In targeted attacks, assailants might resort to social engineering or gain physical access to the victim's computer to carry out the installation. Being vigilant and exercising caution when downloading files or clicking on links from unknown sources is crucial to prevent such attacks and protect one's personal information.


Attacker
Legitimate Program (e.g., Virus cleaner)
binder
Trojan Program (BO2K, NetBus, ..)
–Server
Delivery Channel
Email Server (IMAP, POP...)
Web Server (Apache...)
IM/P2P Networks (IRC...)
Software Distribution (games, updates, patches, ...)
Victim

3.1.1 Working

The Havoc Framework is composed of two sections. The Teamserver manages connected operators, tasks agents, parses callbacks, listeners, downloaded data from agents, and screenshots. In order for known and authorised operators to access it, it should be running on a public VPS.

The Client serves as the server's user interface. You can communicate with the agents there, give them orders, and get results from them.

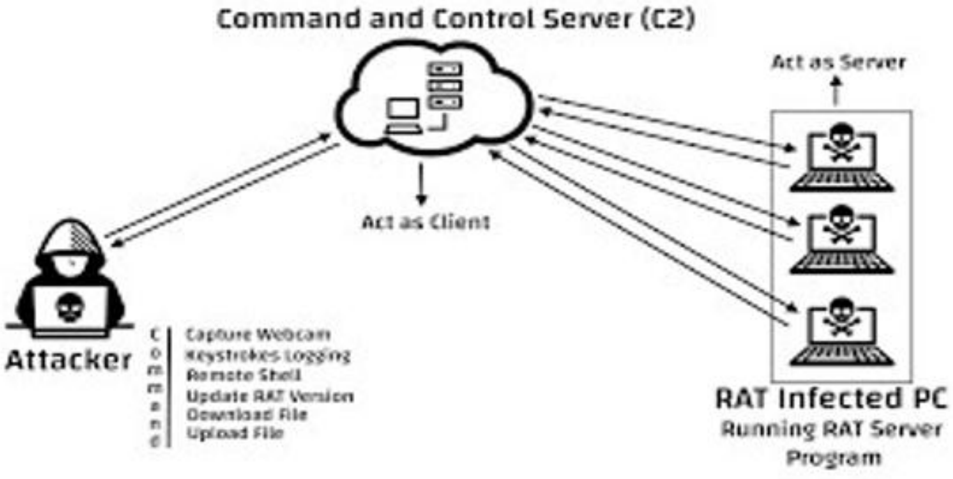


FIGURE: COMMAND AND CONTROL SERVER

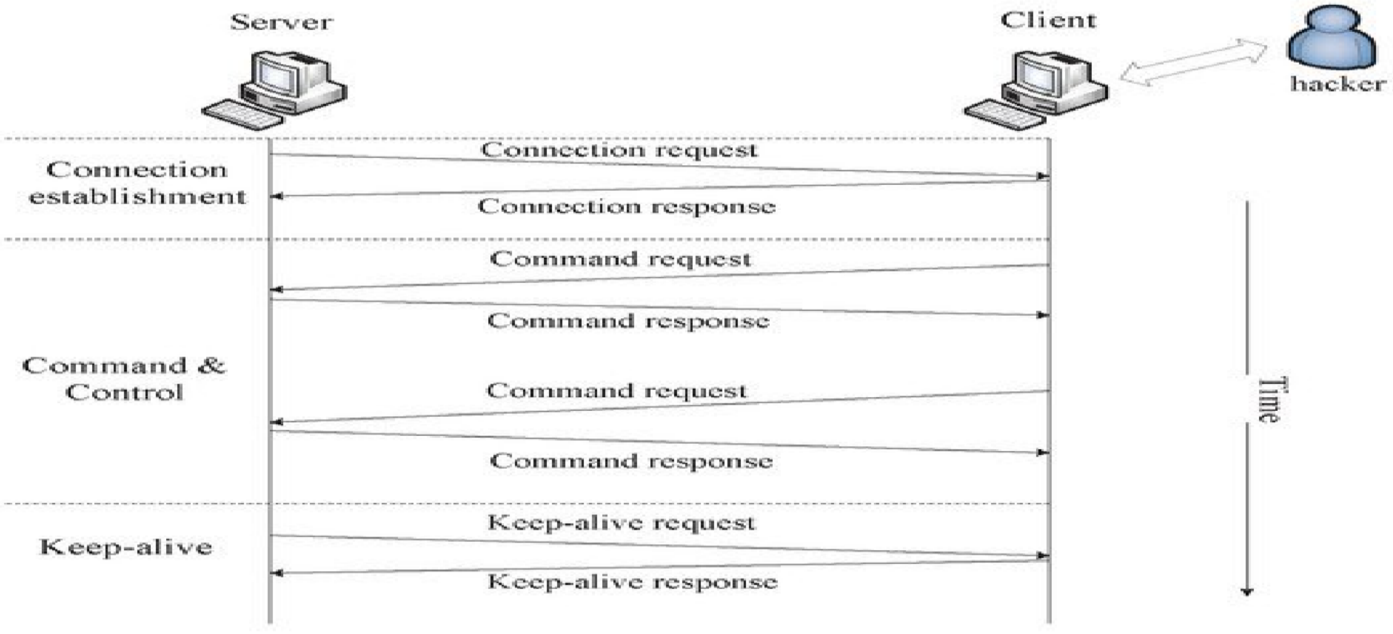


FIGURE: RATS MECHANISM

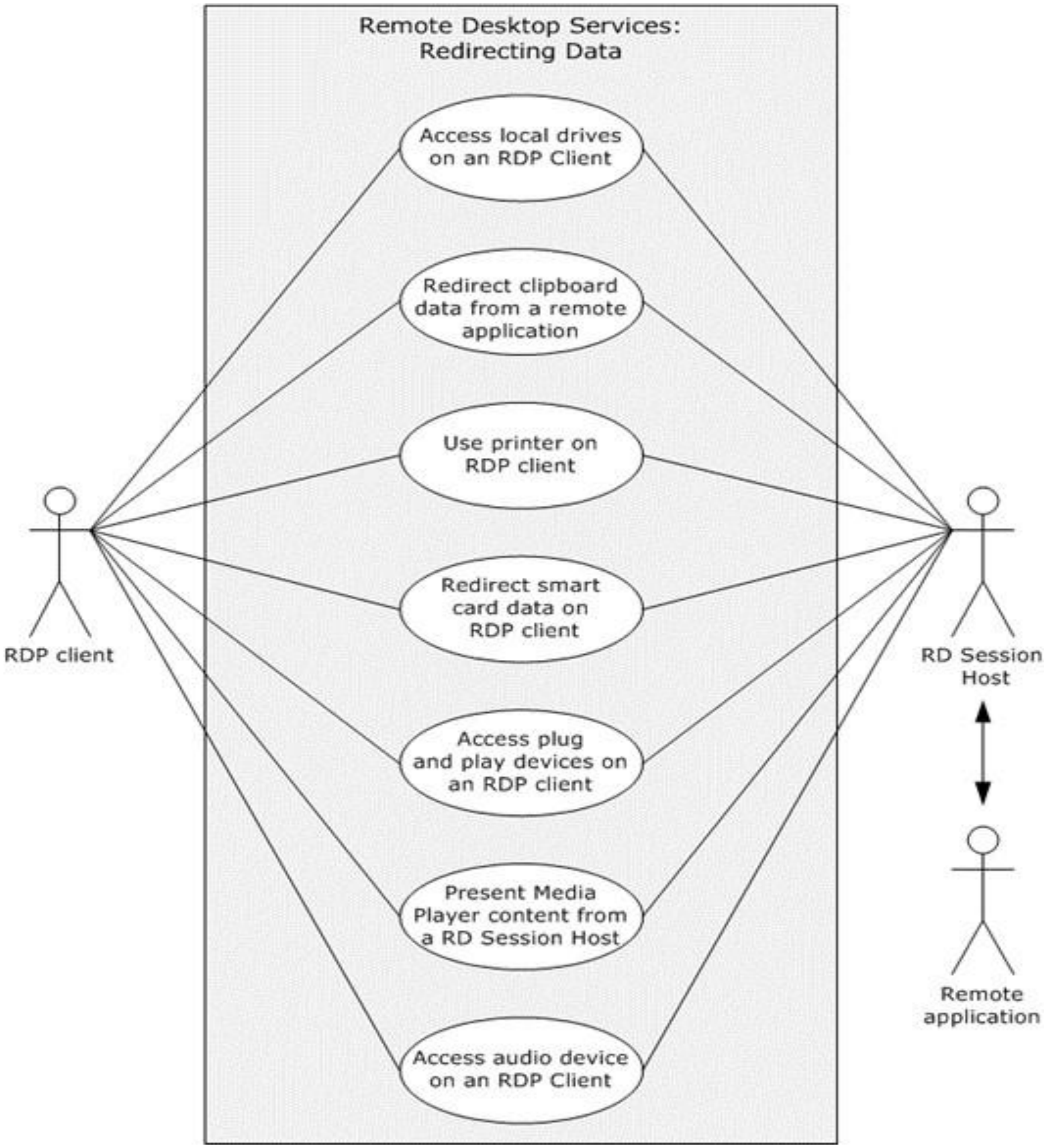

Remote Desktop Services:
Redirecting Data
Access local drives on an RDP Client
Redirect clipboard data from a remote application
Use printer on RDP client
Redirect smart card data on RDP client
Access plug and play devices on an RDP client
Present Media Player content from a RD Session Host
Access audio device on an RDP Client
RDP client
RD Session Host
Remote application

FIGURE: USE CASE DIAGRAM

4 SYSTEM ARCHITECTURE

4.1 Architectural Design

The design chosen for RAS is a layered Client server architecture.

We will have a 3 layered architecture having Presentation, Application and Network Layer.

Presentation Layer: It will handle the view or UI.

Application Layer: It will have all the business logic incorporated.

Network Layer: It will manage the connection and network over which exploitation will take place.

Client Server divides the system into two parts, client and server. Although our solution will be lightweight and efficient, still most of the system operations will be carried out on the Administrative/Server side. API will be installed on both client and server side to perform their respective operations.

Client Side: User will be the main actor on client side, he will use the exploited network and interact with the payload to give away vulnerability.

Server Side: Server/Administrative side of the application is where the administrator creates payload and listen to HTTP/HTTPS. Alongside, it uses payload to exploit network and gain access to client/target device.

The decomposition of the subsystems shown in the architectural design is explained in the following ways.

4.2 Module Decomposition:

The module decomposition is explained through class diagram that depicts all the classes of RAS.

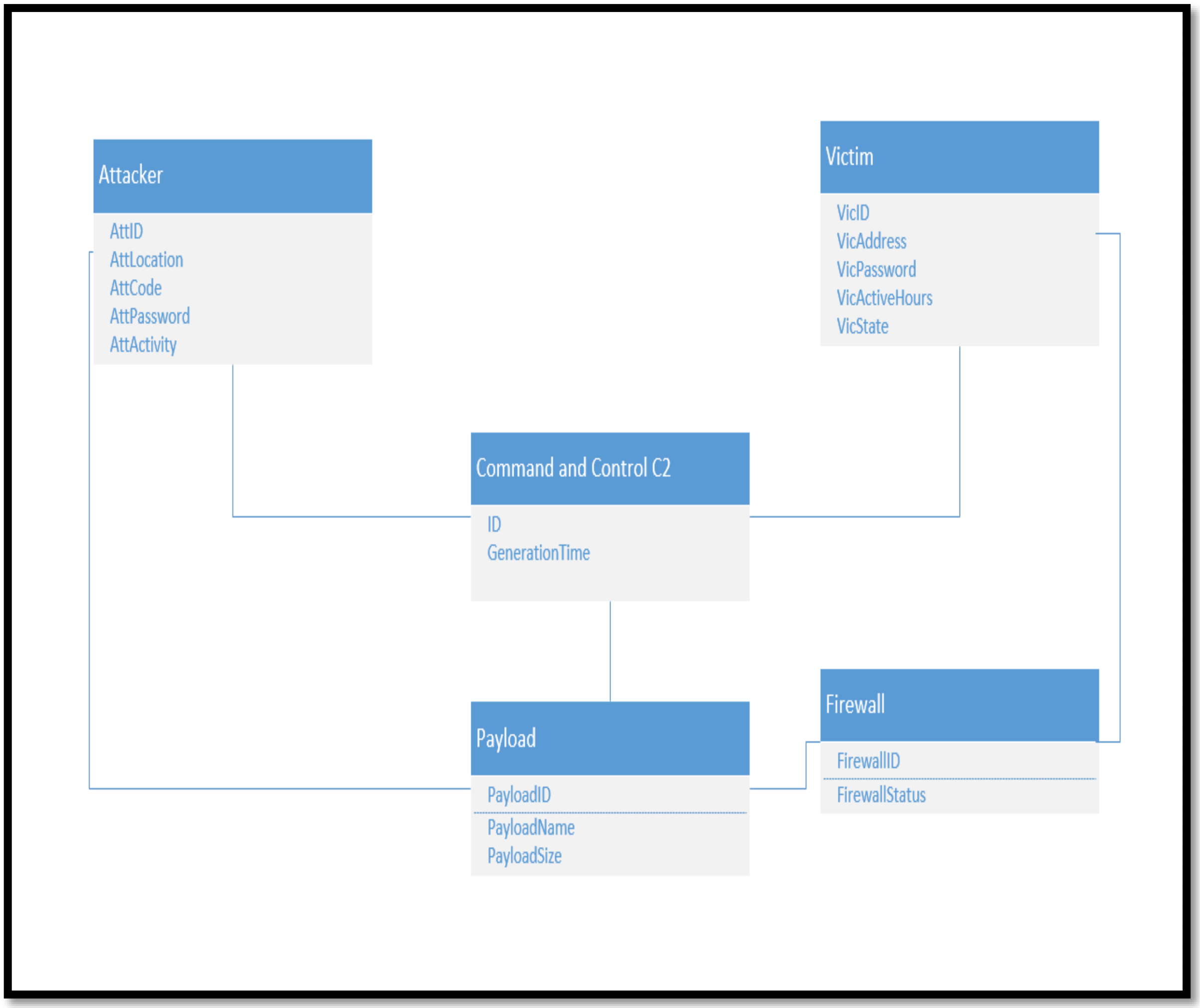


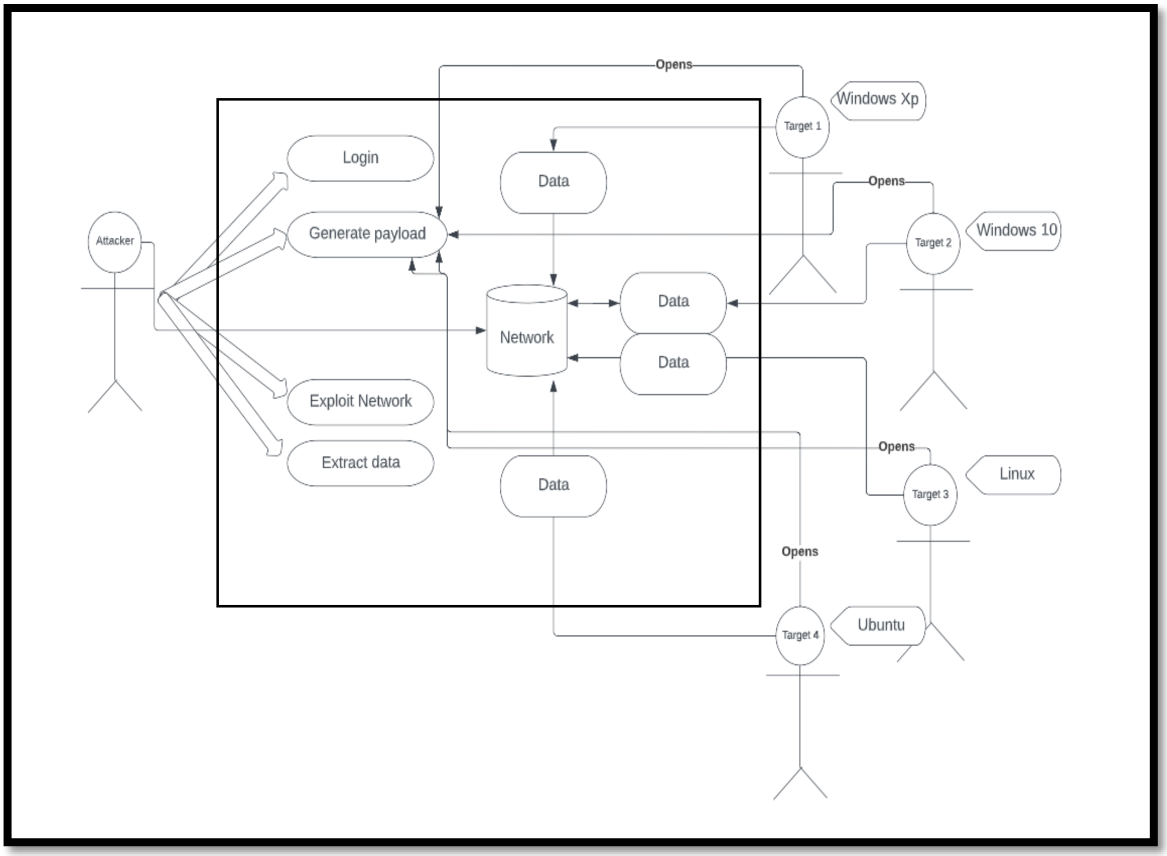
FIGURE: CLASS DIAGRAM

4.3 Process Decomposition

The process decomposition is explained through use case, sequence and activity diagrams which decompose the system into well-defined and cohesive processes. The use cases and the subsequent use case narratives explain the set of actions that a user undertakes while dealing with RAS.

4.3.1 Use Case Diagrams and Use Case Narratives

The use cases and the subsequent use case narratives explain the set of actions that an actor undertakes while dealing with RAS.



1. Login

RAS Use Case 01: Login	
Actors	Admin/Attacker
Pre-condition	Login credentials are valid Dashboard is displayed to user
Trigger	The Actor wants to login his account.
Main Path (Primary Path)	➢ Registered actor enters credentials to login. ➢ Login credentials are validated to authenticate the user. ➢ Authenticated user is redirected to the main interface.
Exception Path	➢ User credentials are invalid and user is not directed to main page
Post-condition	Actor is successfully logged in.

Table 1: RAS Account Login Use case narrative

2. Generate Payload

RAS **Use Case 02:-** **Generate Payload**	
Actors	Admin/Attacker
Pre-condition	➢ File to be used for payload must run on every platform ➢ Payload must be able to break through the defender
Trigger	The actor wants to generate a payload
Main Path (Primary Path)	➢ The attacker generates a payload with Team Server which must be able to exploit the target and make it vulnerable
Exception Path	If user credentials are invalid, the error message is displayed on the screen.
Post-condition	Generated payload can be transferred to any victim to make it vulnerable.

Table 2: Payload Generation Use case narrative

ware

3. Network Exploitation

RAS **Use Case 03: Network Exploitation**	
Actors	Admin/Attacker
Pre-condition	Attacker should be able to access the network remotely through deployed trojan.
Trigger	the attacker wants to exploit the entire network to monitor the network traffic
Main Path (Primary Path)	➢ Using the payload generated through RAS the attacker can exploit the entire network to monitor the network traffic and control it to modify the packets moving through it.
Post-condition	Attacker takes control of the network and can exploit any device connected to the network.

Table 3: Network Exploitation Use case narrative

4. Data Extraction

RAS **Use Case 04: Data Extraction**	
Actors	Admin/Attacker

Pre-condition	User must have opened payload. Payload must have exploited the network/device.
Trigger	The user want to extract data from targeted device.
Main Path **(Primary Path)**	The main purpose of using RAS is to make end-users vulnerable and extract information out of their devices in order to explicitly use it for own purpose or to spy to eliminate threats.
Exception Path	1. Generated payload is unable to exploit the target.
Post-condition	Attacker has control over the entire data of user and can access or extract it whenever required and can monitor every activity of the user

Table 4: Data Extraction Use Case narrative

5. Get Results

RAS Use Case 05: Get Vulnerable	
Actors	User/Target

Pre-condition	The User must be logged in. The user must open payload file and be connected to the exploited network.
Trigger	The user becomes vulnerable to the attack.
Main Path (Primary Path)	The user/target receives the payload and opens it. The payload penetrates through the firewalls of the user device and makes it vulnerable. The data of user is now easily accessible to the attacker.
Post-condition	User becomes vulnerable and all the data of user is easily accessible to the attacker and attacker can monitor the user's every activity.

Table 5: Get Vulnerable Use Case narrative

4.3.2. Sequence Diagram

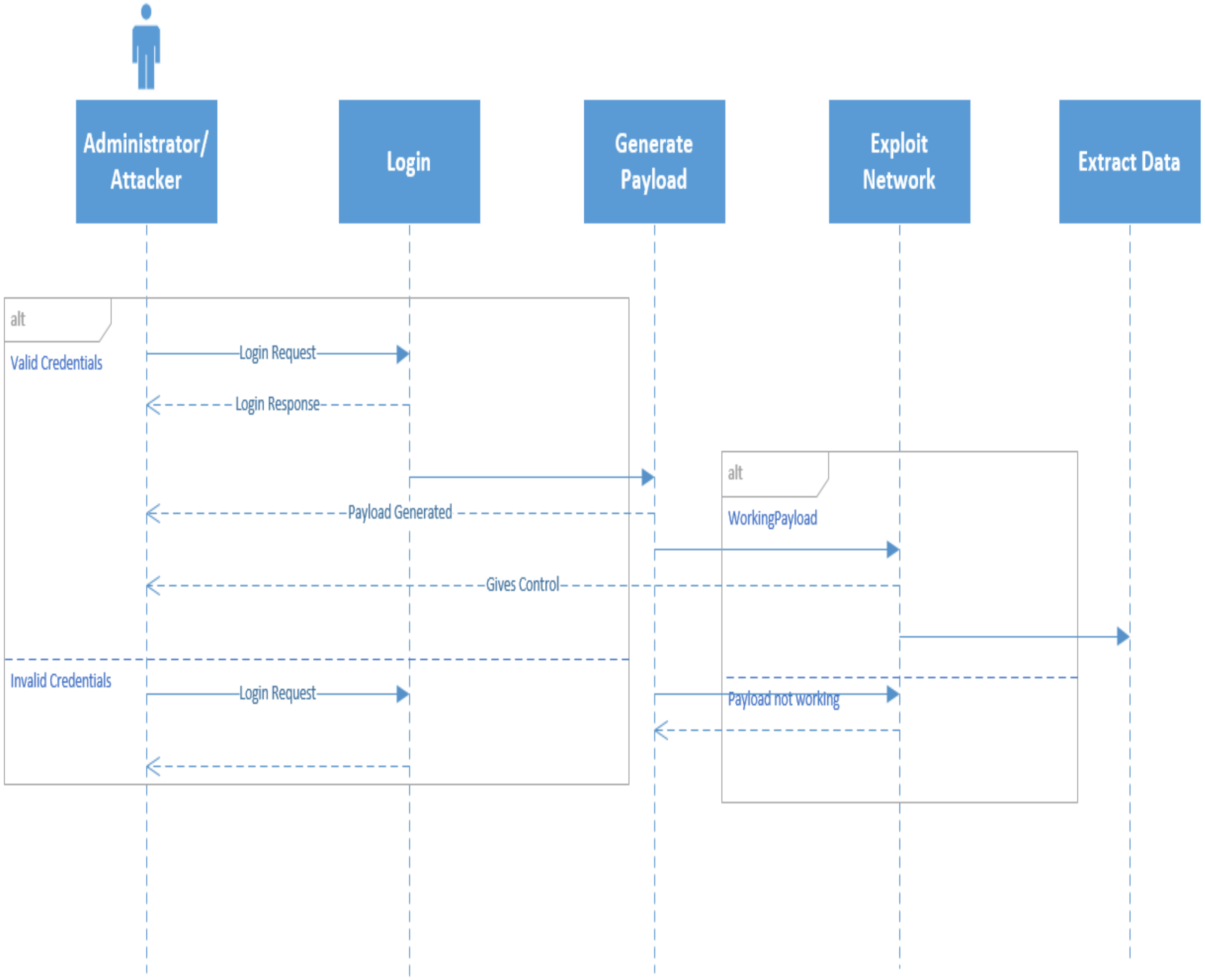


Figure : Sequence Diagram

4.3.3 Activity Diagram

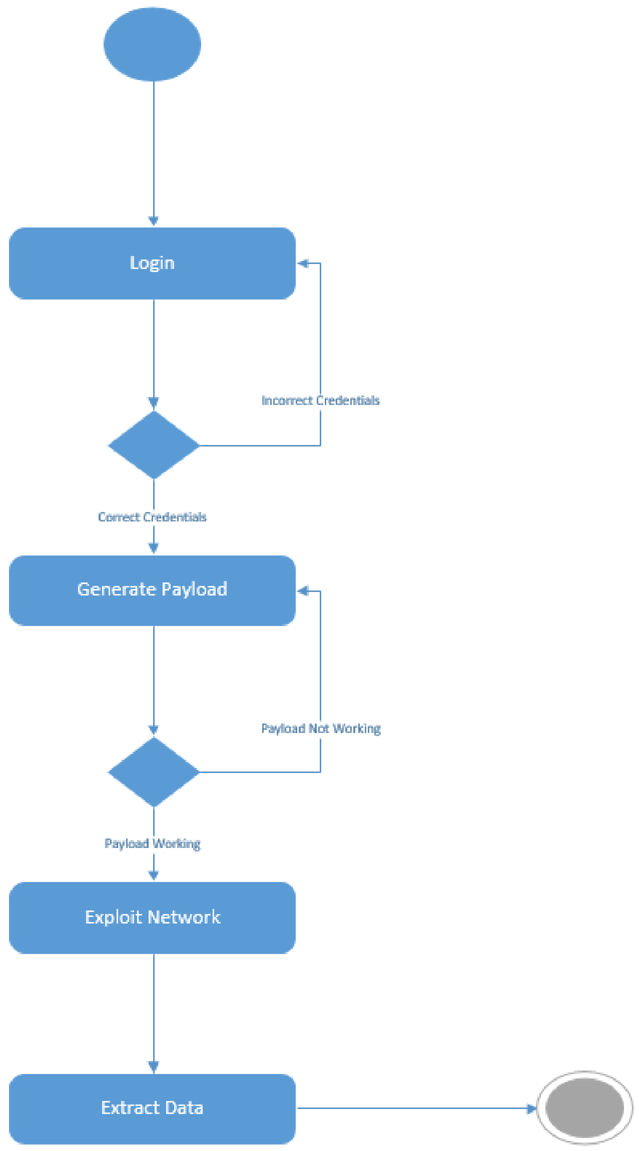


Figure : Activity Diagram

4.3.4 Data Design

4.1 Data Description

A key element of RAS is the storage of data in a real-time database, which lets the administrator to easily access and handle the data gathered from the victim's device. Since data can be immediately stored and retrieved after being collected, the real-time database helps to guarantee that the information is accurate and current.

System logs, network traffic, user passwords, and other metadata that might give important insights into the victim's device usage and behaviour can all be found in the RAS real-time database. Further reconnaissance, targeted assaults, or system vulnerability discovery can all be done using this knowledge.

The preservation and use of such information must, however, adhere to all applicable ethical and legal standards. Any invasion of privacy or unauthorised access to sensitive information might result in serious repercussions, including legal action or reputational harm. To protect the real-time database from unauthorised access or cyberattacks, it is crucial to incorporate strong security measures and access restrictions. Additionally, the database must be used in a morally and responsibly responsible manner.

4.1.1 Database

Important data about the victim's device, administrator account, and network bandwidth can be stored in a database by RAS. This makes it possible for operators to access the data as needed and makes it easier to handle and monitor the victim's device effectively. To avoid any potential misuse or invasion of privacy, it is crucial to stress that the preservation and use of such information should be done in compliance with ethical and legal standards.

5. Component Design

Through the use of a component diagram, each component of the application will be examined in greater detail in this section. The client computer and server, each of which has multiple subcomponents, are the two main components shown in the component diagram.

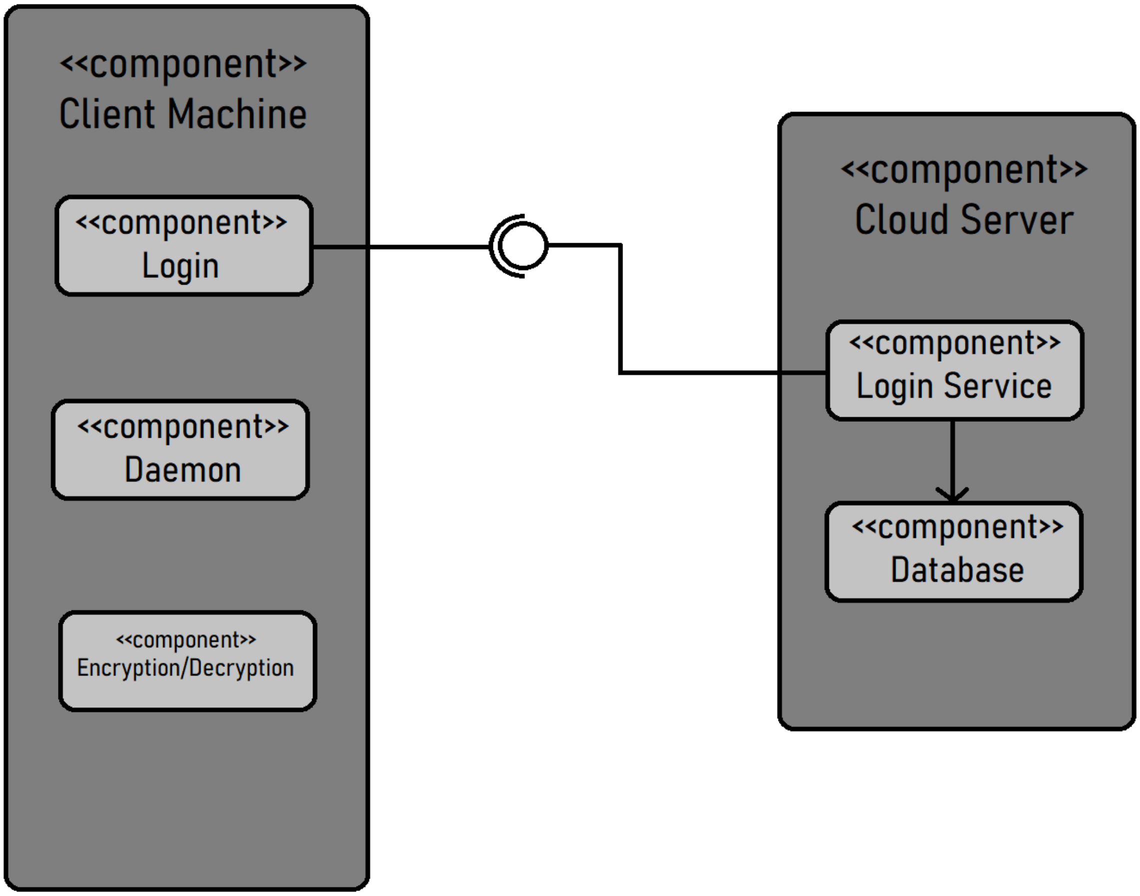
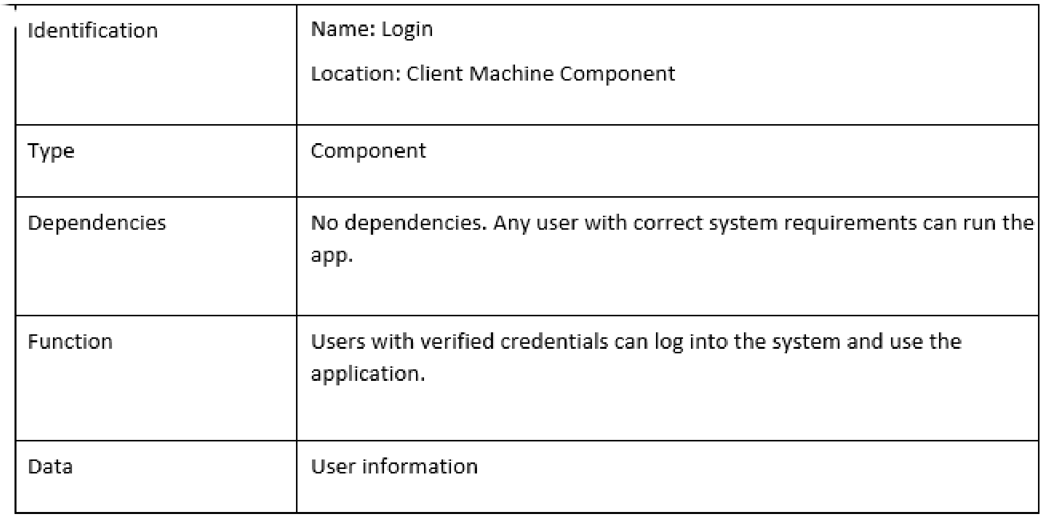


Figure : Component Diagram

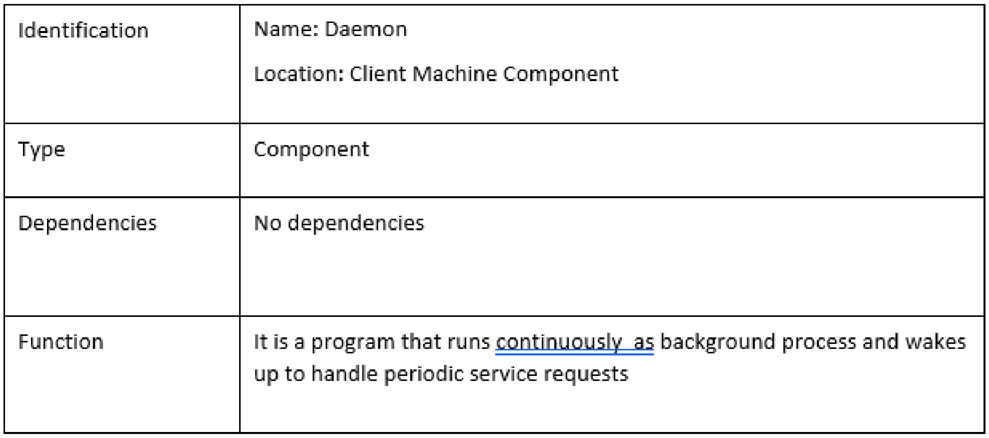
5.1 Client Machine

5.1.1 Login



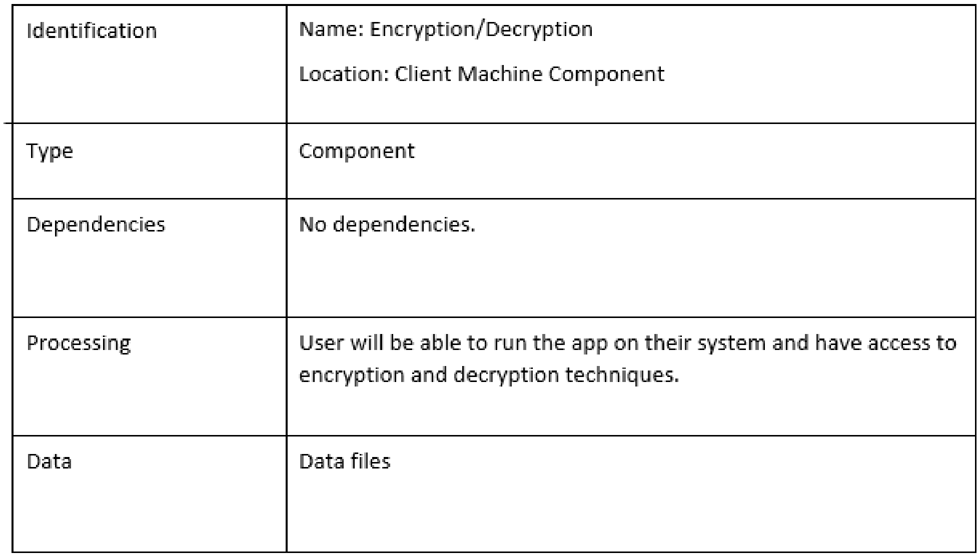
Identification	Name: Login Location: Client Machine Component
Type	Component
Dependencies	No dependencies. Any user with correct system requirements can run the app.
Function	Users with verified credentials can log into the system and use the application.
Data	User information

5.1.2 Daemon



Identification	Name: Daemon Location: Client Machine Component
Type	Component
Dependencies	No dependencies
Function	It is a program that runs continuously as background process and wakes up to handle periodic service requests

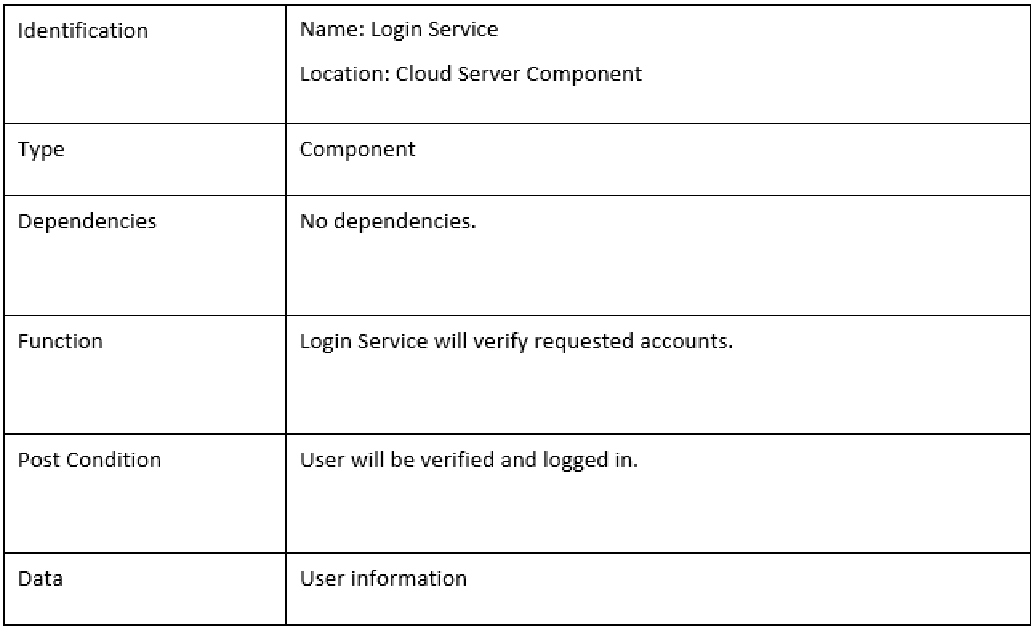
5.1.3 Encryption/Decryption



Identification	Name: Encryption/Decryption Location: Client Machine Component
Type	Component
Dependencies	No dependencies.
Processing	User will be able to run the app on their system and have access to encryption and decryption techniques.
Data	Data files

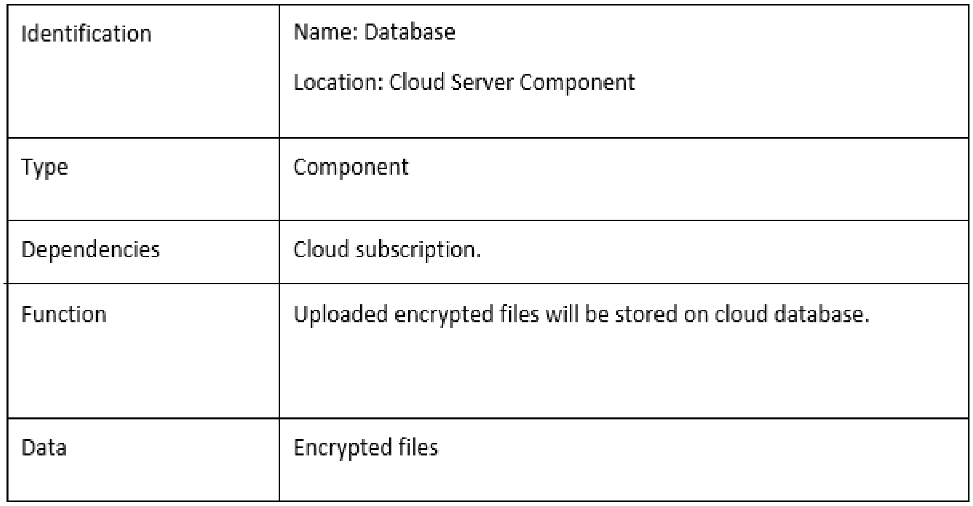
5.2 Cloud Server

5.2.1 Login Service



Identification	Name: Login Service Location: Cloud Server Component
Type	Component
Dependencies	No dependencies.
Function	Login Service will verify requested accounts.
Post Condition	User will be verified and logged in.
Data	User information

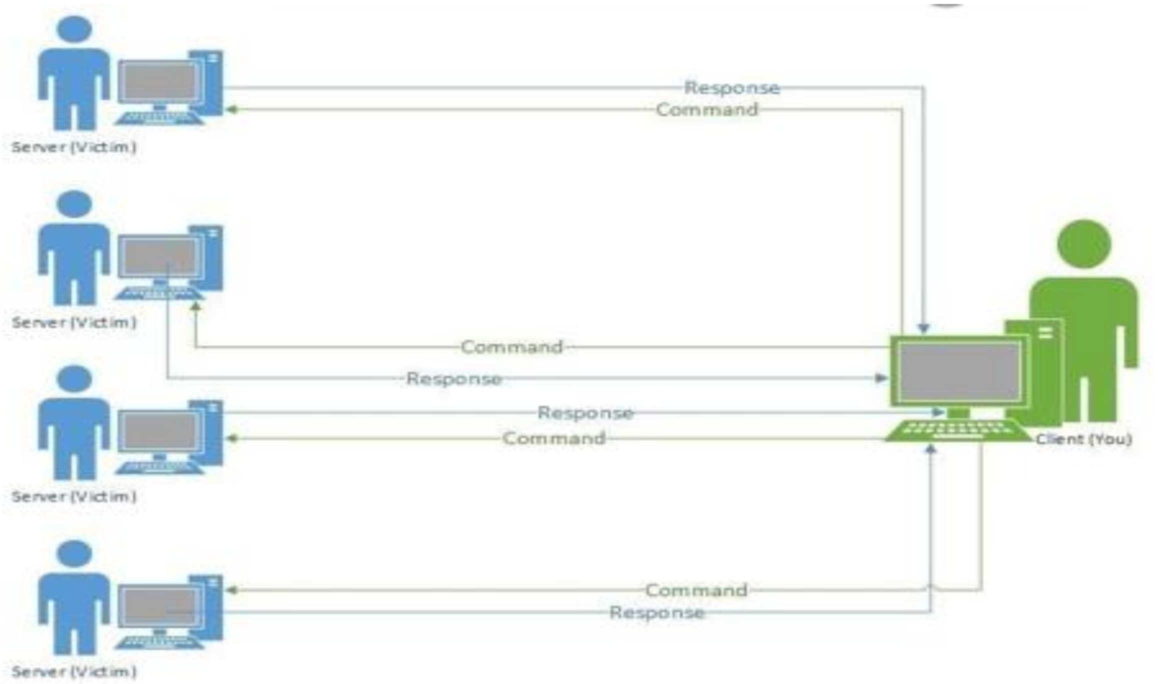
5.2.2 Database

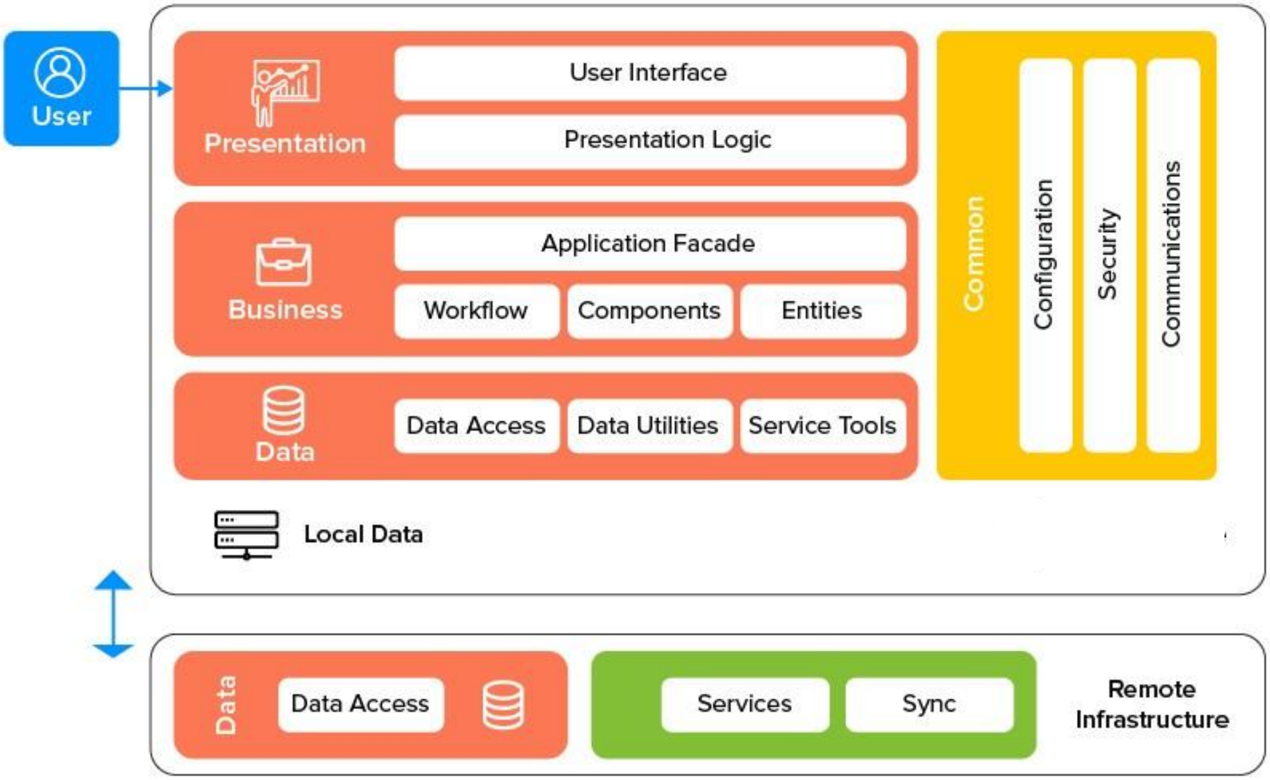


Identification	Name: Database Location: Cloud Server Component
Type	Component
Dependencies	Cloud subscription.
Function	Uploaded encrypted files will be stored on cloud database.
Data	Encrypted files

Code for Desktop Interface:

The Havoc Client user interface is written in Qt and C++ and applied with Dracula theme. The interface is split into three parts .The interface shows visualization of sessions in table or node graph, event viewer and other features.





The three-layer architecture is a widely used multilayer architecture that is crucial in designing application architecture. It pertains to the internal architecture of the application's components. Following constitute the architecture design:

Presentation Layer

This layer focuses on the end-user experience and includes the User Interface and UI process. During this stage, developers need to make important decisions regarding the application's themes, fonts, colours, and data format. It is also necessary to ensure compliance with the client's deployment restrictions.

Business Layer

This layer is responsible for handling the application's business logic and includes components, workflows, and entities. It is technically more complex than others and involves solving various problems, such as caching, exception management and logging. To simplify , further divided into domain model and service layer.

Data Access Layer

It is designed to meet the application's needs and provides proefficient and secured transactions of data. It includes , data access components, service agents and data utility. It is crucial to selecting the right data formats and implement robust validation techniques. Developers should also consider maintaining the data to ensure it remains adaptable to changing business techniques requirements.

Factors to Consider Developing of Architecture

Building a solid application architecture is crucial for achieving success in software development. It's important to keep a record of any mistakes made during the architecture design process, as this can help prevent future failures. Neglecting important factors or avoiding potential problems can result in a failed application. To ensure success, there are several important considerations to keep in mind when developing an architecture:

1. Keep track of mistakes: It is important to keep track of mistakes made during software development architecture. This helps in identifying and fixing the problems to prevent them from happening again in the future.
2. Consider the factors: It is important to consider the factors that can impact the architecture of your application. Some factors to consider include scalability, security, usability, and maintainability.
3. Avoid common pitfalls: Avoiding common pitfalls is essential in creating a successful application architecture. Some common pitfalls to avoid include over-engineering, under-engineering, not testing the architecture, and not validating the architecture with stakeholders.
4. Prioritize simplicity: Simplicity is key in application architecture. Overly complex architectures can lead to issues in maintenance, scalability, and overall success of the application.
5. Focus on flexibility: Flexibility is important in application architecture as business needs can change rapidly. A flexible architecture allows for easy modifications and adaptations to meet changing needs.
6. Collaborate with stakeholders: Collaboration with stakeholders is crucial in developing an application architecture that meets the needs of the business and end-users. Stakeholders can provide valuable feedback and insights that can help in creating a successful architecture.

Determination of the Device Type

Determining device types is another important factor . The operating system decides the type of computers. They are based on the operating system in use. Besides the categories or device type , you should consider many other things. Other things include screen size, resolution, and CPU characteristics. Furthermore, consider availability of development tool framework and storage capacity.

Bandwidth Scenario

The internet connectivity bandwidth of your target audience is a significant aspect to consider when developing software. It's essential to factor in scenarios where there might be no connectivity, and ensure that your app performs well on users' internet, as they may abandon your software if it's slow. Therefore, you should consider factors such as access mechanism,speed,and account power consumption and opt the best software protocols and hardware. Additionally, you need to tailor these factors to accommodate slow and intermittent internet connections.

User Interface

A well-designed user interface is a crucial aspect of software development. It enhances the user experience by facilitating easy and comfortable interaction with the app. The interface should be intuitive and visually appealing, devoid of any ambiguity or complexity. The more intuitive and visually appealing it is, the stronger the connection between the app and the users. To ensure maximum effectiveness, the interface design should be tailored to the specific needs and preferences of the target audience.

Right Navigation Method

Selecting appropriate navigation method is an important aspect of software development that can greatly impact user experience. Therefore, it is important to analyze various navigation methods and choose the suitable most based on the requirements desired and customers’ preference.Some of the commonly used navigation methods include:

Tab Controller

One can switch between the groups of tabs with links **Real-Time Updates vs. Push**

Stacked Navigation Bar

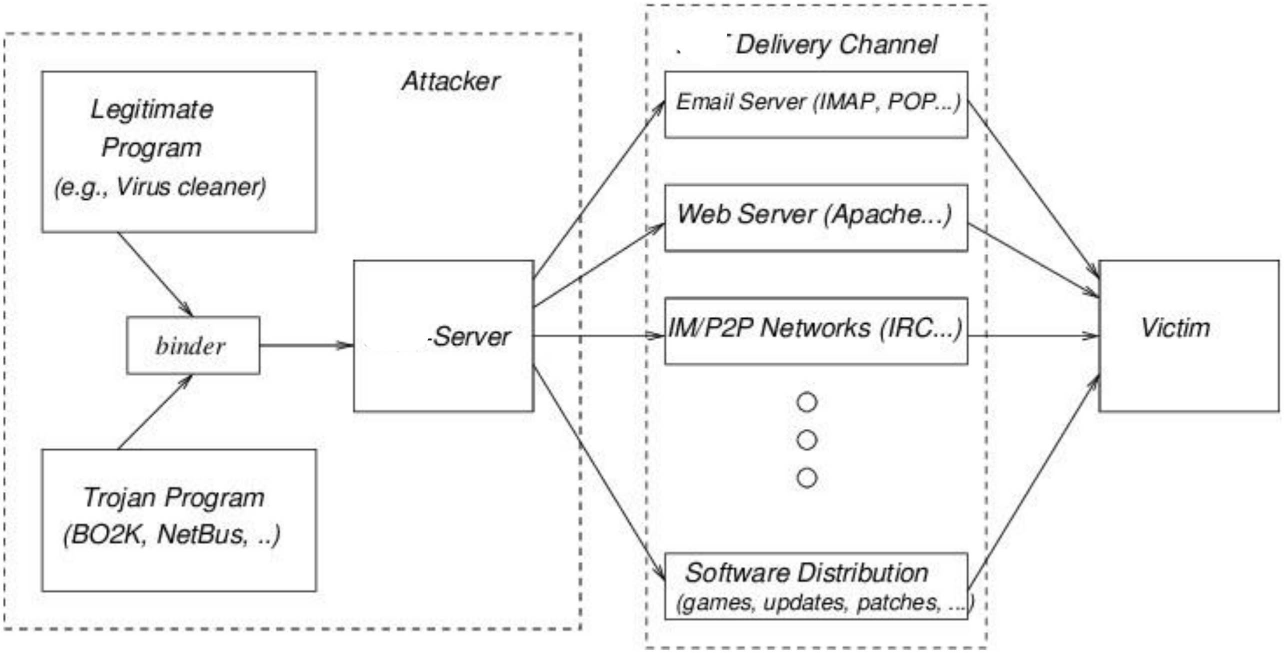
In this,there is the design of a fixed bar. You put their links with respect to all other elements within the software.

Notifications

It is important to consider whether to incorporate real-time updates or push button functionality into your software. Your decision should be based on your target audience and their needs. Real-time updates might be expensive to implementation but offers a feature which enhances user experience.

4.2 Decomposition Description

Trojan Binding and Encryption


Attacker
Legitimate Program (e.g., Virus cleaner)
binder
Trojan Program (BO2K, NetBus, ..)
Server
Delivery Channel
Email Server (IMAP, POP...)
Web Server (Apache...)
IM/P2P Networks (IRC...)
Software Distribution (games, updates, patches, ...)
Victim

Design Rationale

The design of RAS was chosen for several reasons.

- Firstly, it performs specific tasks and provides security through crypting systems.
- Secondly, it is low cost compared to other tools available on the market.
- Thirdly, it performs tasks within a specific time frame.
- Fourthly, RAS requires low data bandwidth consumption.
- Fifthly, the efficiency level of generated payloads is high.
- Sixthly, RAS has a minimal user interface and is easy to use.
- Lastly, RAS requires little to no human intervention.

5 DATA DESIGN

5.1 Data Description

RAS is an advanced and customizable post-exploitation command and control framework, providing users with a range of features to monitor and establish command and control frameworks. With its intuitive and user-friendly GUI, RAS offers a sleek interface and additional exciting features that set it apart from its competitors. Users can create custom backdoors or bind the payload with a social media or gaming app. This unique flexibility allows users to tailor the RAS framework to meet their specific needs and requirements. Overall, RAS provides a powerful tool for monitoring and controlling systems and is an excellent choice for those seeking advanced features and customization options.

Sure! Here are some additional details about each feature:

1. Easy to use GUI interface: The user interface is to be designed for being user-friendly and intuitive, for making it easy to navigate the app and accessing features.

2. Simple payload generator: The app allows users to create custom backdoor payloads or bind payloads with existing attachments with ease.

3. Powerful Files Explorer with all access privileges: Users have complete access to the device's file system, allowing them to explore files and folders, copy, move, delete, and perform other file operations remotely.

4. Read and Write Messages remotely: The app enables users to view and send messages from the target device without physical access to the device.

5. Browse Call Logs: Users can browse the call logs of the target device remotely and view detailed call information.

6. Read/Write Contact List: Users can remotely view and manage the contact list of the target device.

7. Remote Camera to capture Images & Videos from target device: Users can remotely capture photos and videos from the target device's camera.

8. Listen to the live conversations through remote Mic, and record the audio from Mic: The app allows users to listen to live conversations through the target device's microphone and record audio.

9. Check Internet Browser History: Users can remotely view the internet browsing history of the target device.

10. GPS Locator: Users can track the location of the target device remotely using its GPS.

11. List of all the installed Applications: The software provides users with a list of all the applications installed on the target device.

12. Get phone’s detailed info: Users can view detailed information about the target device, such as the device's model, operating system, storage capacity, etc.

13. FULLY STEALTH MODE..!: Operates in stealth mode, allowing users to monitor the target device without the user's knowledge.

14. Pivoting: The app supports pivoting, allowing users to route their connection through the target device to gain access to other devices on the same network.

15. Listeners: The app supports listeners, allowing users to listen for incoming connections on multiple ports simultaneously.

16. Multi port support: Can work on any port: Can be configured to work on any port, providing flexibility in network configurations.

17. Insertion point encoding: The app supports insertion point encoding, allowing users to obfuscate their payloads to avoid detection.

18. Run multiple patches on a single device: Users can run multiple patches on a single device to perform various operations simultaneously.

19. Transmit data securely from and to the device over the network: Uses secure encryption protocols to transmit data between the target device and the user's device.

20. Capable of controlling program configurations: Users can configure the to suit their specific needs and preferences.

21. Notifications hidden from the phone’s notification bar: Operates in stealth mode and hides all notifications from the target device's notification bar.

22. Name of the package can be changed to anything: Users can change the name of the package to avoid detection by anti-virus software.

Before installing the RAS, customization is done,and attaching it with a genuine attachment, game, or software to make it more believable. The most effective way to create a trojan is by coding it via terminal and converting it into an executable. For DDos attacks, trojans are spread on multiple computers, and attackers can randomly select active users on chat platforms to inject the trojan into their system. Once injected, it can survive reboots, evade anti-viruses on the target and system crash. It can edit files and registry and can be transparently triggered once it reboots everytime .

6 HUMAN INTERFACE DESIGN

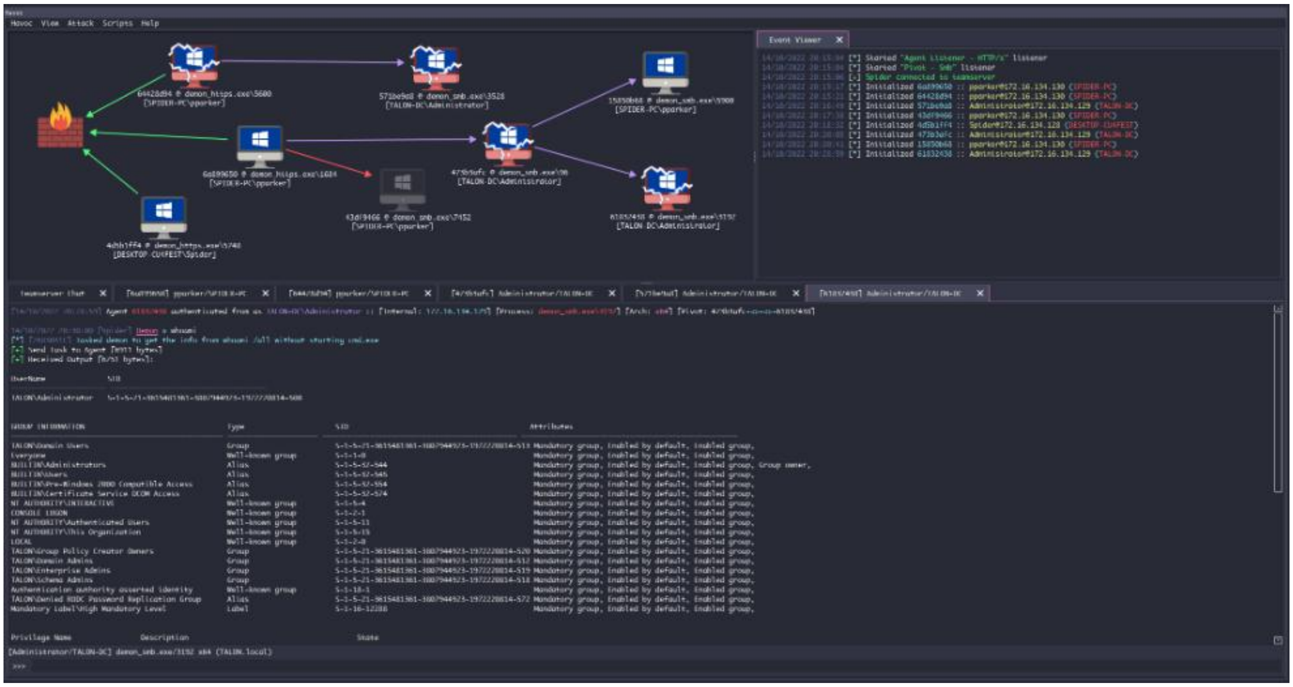
6.1 Overview : User Interface

In this project, human user interface is Software based.Meaning that the point where the user will interact with our device is totally based on Software using a Desktop Interface. So, to easily understand the user interface design, following points will help a lot.

1. The Desktop Interface will be started on desktop. 2.
   UDP/TCP port will be given before executing
3. The payload will be generated and obsfucated.

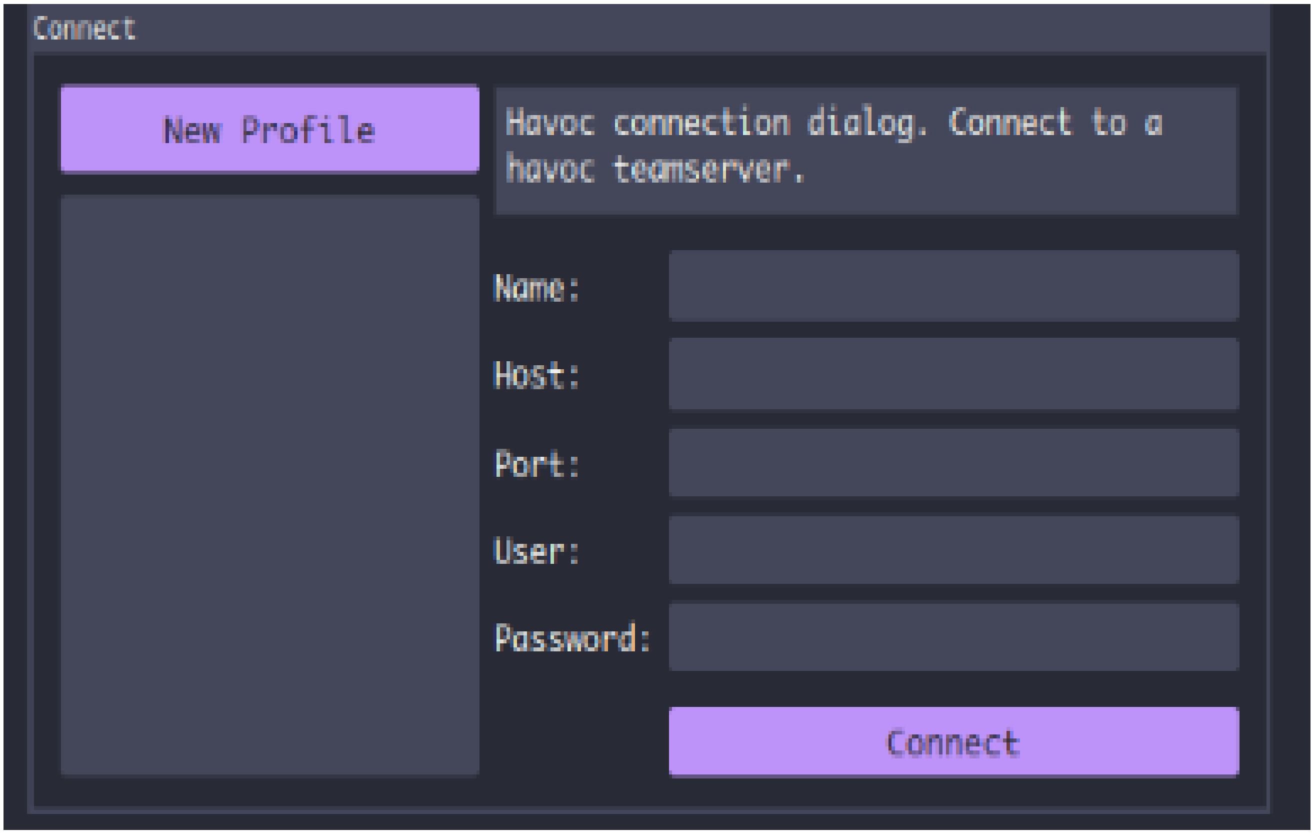
So, in this way, after Creating a payload our Trojan is ready to exploit any device in the network.

6.2 Interface Images


Havoc
Havoc View Attack Scripts Help
64428d94 @ demon_https.exe\5600
[SPIDER-PC\pparker]
571be9a8 @ demon_smb.exe\3528
[TALON-DC\Administrator]
15850b68 @ demon_smb.exe\5908
[SPIDER-PC\pparker]
6a899650 @ demon_https.exe\1604
[SPIDER-PC\pparker]
473b3afc @ demon_smb.exe\98
[TALON-DC\Administrator]
43df9466 @ demon_smb.exe\7452
[SPIDER-PC\pparker]
61832438 @ demon_smb.exe\3192
[TALON-DC\Administrator]
4d5b1ff4 @ demon_https.exe\5740
[DESKTOP-CUXFEST\Spider]
Event Viewer
Teamserver Chat
[6a899650] pparker/SPIDER-PC
[64428d94] pparker/SPIDER-PC
[473b3afc] Administrator/TALON-DC
[571be9a8] Administrator/TALON-DC
[61832438] Administrator/TALON-DC

```
14/10/2022 20:15:04 [*] Started "Agent Listener - HTTP/s" listener
14/10/2022 20:15:04 [*] Started "Pivot - Smb" listener
14/10/2022 20:15:06 [+] Spider connected to teamserver
14/10/2022 20:15:17 [*] Initialized 6a899650 :: pparker@172.16.134.130 (SPIDER-PC)
14/10/2022 20:15:21 [*] Initialized 64428d94 :: pparker@172.16.134.130 (SPIDER-PC)
14/10/2022 20:16:49 [*] Initialized 571be9a8 :: Administrator@172.16.134.129 (TALON-DC)
14/10/2022 20:17:38 [*] Initialized 43df9466 :: pparker@172.16.134.130 (SPIDER-PC)
14/10/2022 20:18:32 [*] Initialized 4d5b1ff4 :: Spider@172.16.134.128 (DESKTOP-CUXFEST)
14/10/2022 20:20:08 [*] Initialized 473b3afc :: Administrator@172.16.134.129 (TALON-DC)
14/10/2022 20:20:41 [*] Initialized 15850b68 :: pparker@172.16.134.130 (SPIDER-PC)
14/10/2022 20:28:59 [*] Initialized 61832438 :: Administrator@172.16.134.129 (TALON-DC)
```

```
[14/10/2022 20:28:59] Agent 61832438 authenticated from as TALON-DC\Administrator :: [Internal: 172.16.134.129] [Process: demon_smb.exe\3192] [Arch: x64] [Pivot: 473b3afc-<-<-<-61832438]

14/10/2022 20:30:00 [Spider] Demon » whoami
[*] [0A39D43C] Tasked demon to get the info from whoami /all without starting cmd.exe
[+] Send Task to Agent [8911 bytes]
[+] Received Output [8/51 bytes]:

UserName              SID
===================== ============================================
TALON\Administrator   S-1-5-21-3815481361-3007944923-1972220814-500


GROUP INFORMATION                              Type              SID                                            Attributes
============================================== ================= ============================================== ==========================================
TALON\Domain Users                             Group             S-1-5-21-3815481361-3007944923-1972220814-513 Mandatory group, Enabled by default, Enabled group,
Everyone                                       Well-known group  S-1-1-0                                        Mandatory group, Enabled by default, Enabled group,
BUILTIN\Administrators                         Alias             S-1-5-32-544                                   Mandatory group, Enabled by default, Enabled group, Group owner,
BUILTIN\Users                                  Alias             S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group,
BUILTIN\Pre-Windows 2000 Compatible Access     Alias             S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group,
BUILTIN\Certificate Service DCOM Access        Alias             S-1-5-32-574                                   Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\INTERACTIVE                       Well-known group  S-1-5-4                                        Mandatory group, Enabled by default, Enabled group,
CONSOLE LOGON                                  Well-known group  S-1-2-1                                        Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\Authenticated Users               Well-known group  S-1-5-11                                       Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\This Organization                 Well-known group  S-1-5-15                                       Mandatory group, Enabled by default, Enabled group,
LOCAL                                          Well-known group  S-1-2-0                                        Mandatory group, Enabled by default, Enabled group,
TALON\Group Policy Creator Owners              Group             S-1-5-21-3815481361-3007944923-1972220814-520 Mandatory group, Enabled by default, Enabled group,
TALON\Domain Admins                            Group             S-1-5-21-3815481361-3007944923-1972220814-512 Mandatory group, Enabled by default, Enabled group,
TALON\Enterprise Admins                        Group             S-1-5-21-3815481361-3007944923-1972220814-519 Mandatory group, Enabled by default, Enabled group,
TALON\Schema Admins                            Group             S-1-5-21-3815481361-3007944923-1972220814-518 Mandatory group, Enabled by default, Enabled group,
Authentication authority asserted identity     Well-known group  S-1-18-1                                       Mandatory group, Enabled by default, Enabled group,
TALON\Denied RODC Password Replication Group   Alias             S-1-5-21-3815481361-3007944923-1972220814-572 Mandatory group, Enabled by default, Enabled group,
Mandatory Label\High Mandatory Level           Label             S-1-16-12288                                   Mandatory group, Enabled by default, Enabled group,


Privilege Name            Description                     State
[Administrator/TALON-DC] demon_smb.exe/3192 x64 (TALON.local)
>>>
```



Havoc connection dialog. Connect to a havoc teamserver.

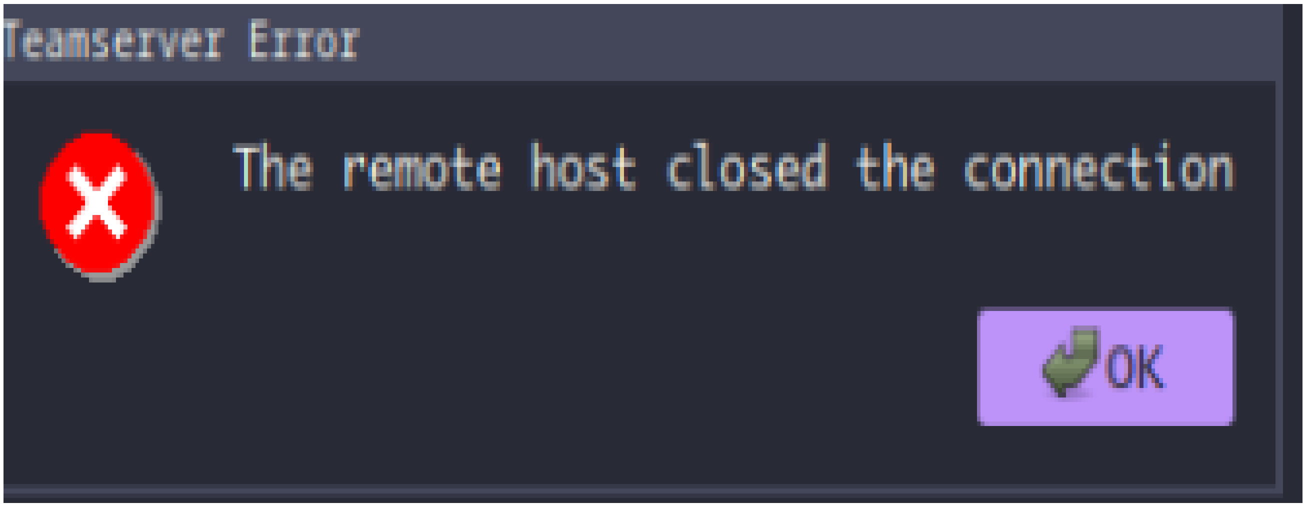
Name:

Host:

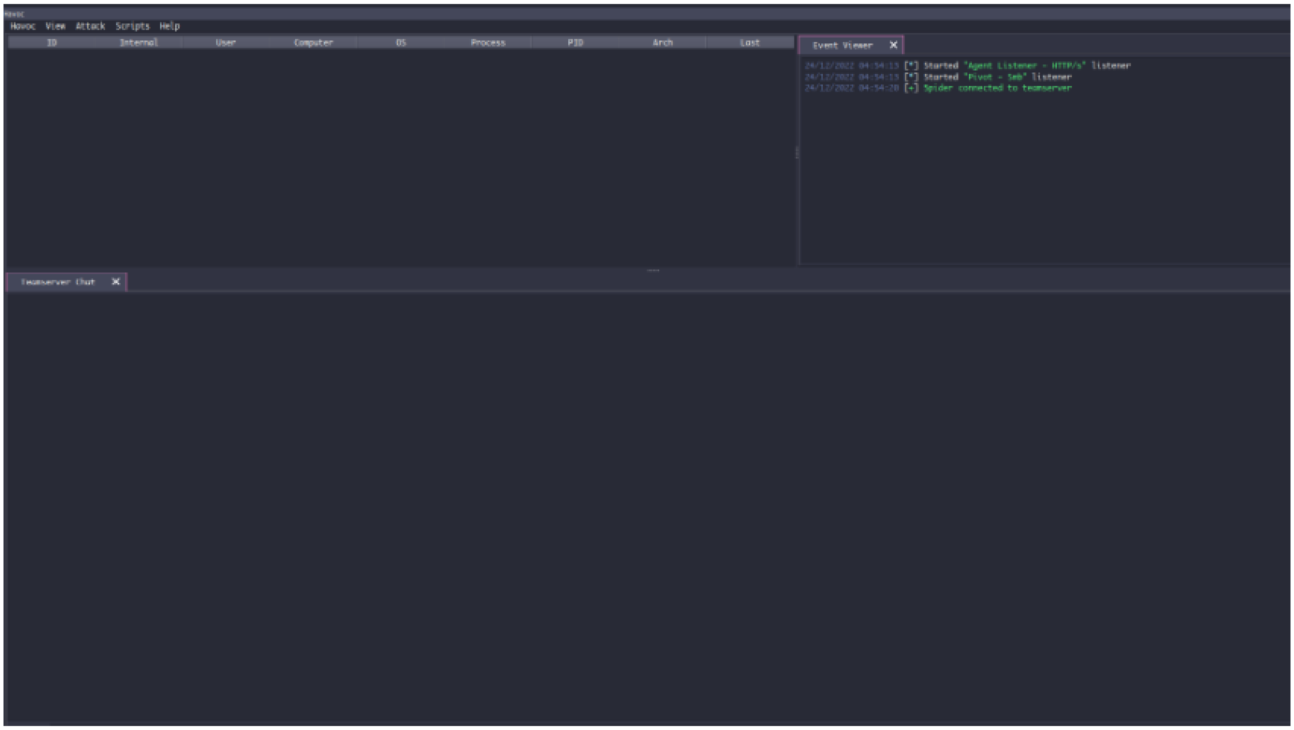
Port:

User:

Password:



The remote host closed the connection



```
24/12/2022 04:54:13 [*] Started "Agent Listener - HTTP/s" listener
24/12/2022 04:54:13 [*] Started "Pivot - Smb" listener
24/12/2022 04:54:20 [+] Spider connected to teamserver
```

Chapter 7: Conclusion

In this thesis, we have described Remote Administrative Software which gives you the power to establish control over devices with a userfriendly GUI and all the features needed for monitoring them. Build customized backdoor payloads or binding the payloads with any of the existing attachments.

1. User-friendly Graphical User Interface.
2. Payload generator with a simple interface.
3. Comprehensive Files Explorer with full access privileges.
4. Remote reading and writing of messages.
5. Pivoting capabilities.
6. Listeners for remote control.
7. Access to Call Logs for browsing.
8. Access to Contact List for reading and writing.
9. Remote Camera feature for capturing images and videos from the target device.
10. Live audio recording from remote Mic and listening to live conversations.
11. Capability to check Internet Browser History.
12. GPS Locator feature.
13. Detailed list of all the installed Applications.
14. Detailed information about the phone.
15. Fully stealth mode for complete anonymity.
16. Multi-port support for working on any port.
17. Encoding of insertion points for enhanced security.
18. Capability to run multiple patches on a single device.
19. Secure transmission of data over the network.
20. Control over program configurations.
21. Hidden notifications in the notification bar for complete stealth.
22. Capability to change the package name to any desired name.

Before installing trojans are customized , portraying them to be a legitimate source or making it believable.To code via terminal is the most efficient and converting it into executable. RAS once injected in the device can outlive reboots ,evade Anti viruses and system crash.

Chapter 8: Future Work

To commercialize this project, the following future milestones need to be achieved:

1. Developing a software that can be used by law enforcement agencies, intelligence, and surveillance of selected targets, inclusive of terrorists and anti-state factors.

2. Ensure that the RAS possesses the following characteristics:

- The ability to manipulate processes in task manager.
- The ability to hinder mouse movement randomly.
- The ability to delete, move, and download files without permission.
- The ability to infect systems with viruses, malwares, and worms.
- The ability to stop the victim's keyboard from working.
- Provide anytime access to the victim's computer.
- Ensure that the RAS is suitable for security, intelligence, surveillance, and educational purposes.

REFERENCES

1. Canfora, G., & Visaggio, C. A. (2017). Detecting malicious Remote Access Tools: The value of feature selection techniques. Information and Software Technology, 91, 161-178.
2. Kierkegaard, P., & Stinson, E. (2017). Remote Access Tools in Cyber Criminal Operations: A Comparison of the Availability and Pricing of RATs on the Underground Market. In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 441-449). IEEE.
3. Ngo, T., Le-Khac, N. A., & M-Tahir, M. (2017). A survey of popular RATs for Windows. Journal of Information Security and Applications, 34, 46-57.
4. Sylvestre, G., Gagné, M., & Bérubé, J. F. (2018). Exploring the dark side of remote access tools: An empirical study of RATs availability and usage. Computers & Security, 78, 334-347.

Bibliography

6.1 Definitions, Acronyms and Abbreviations

Appendix A: Glossary

6.1.1 Definitions

- Administrative – relating to running of a business..

- End Users – who uses in person or is intended to use the product.

- Exploitation – act of treating someone unfairly in order to benefit you own self

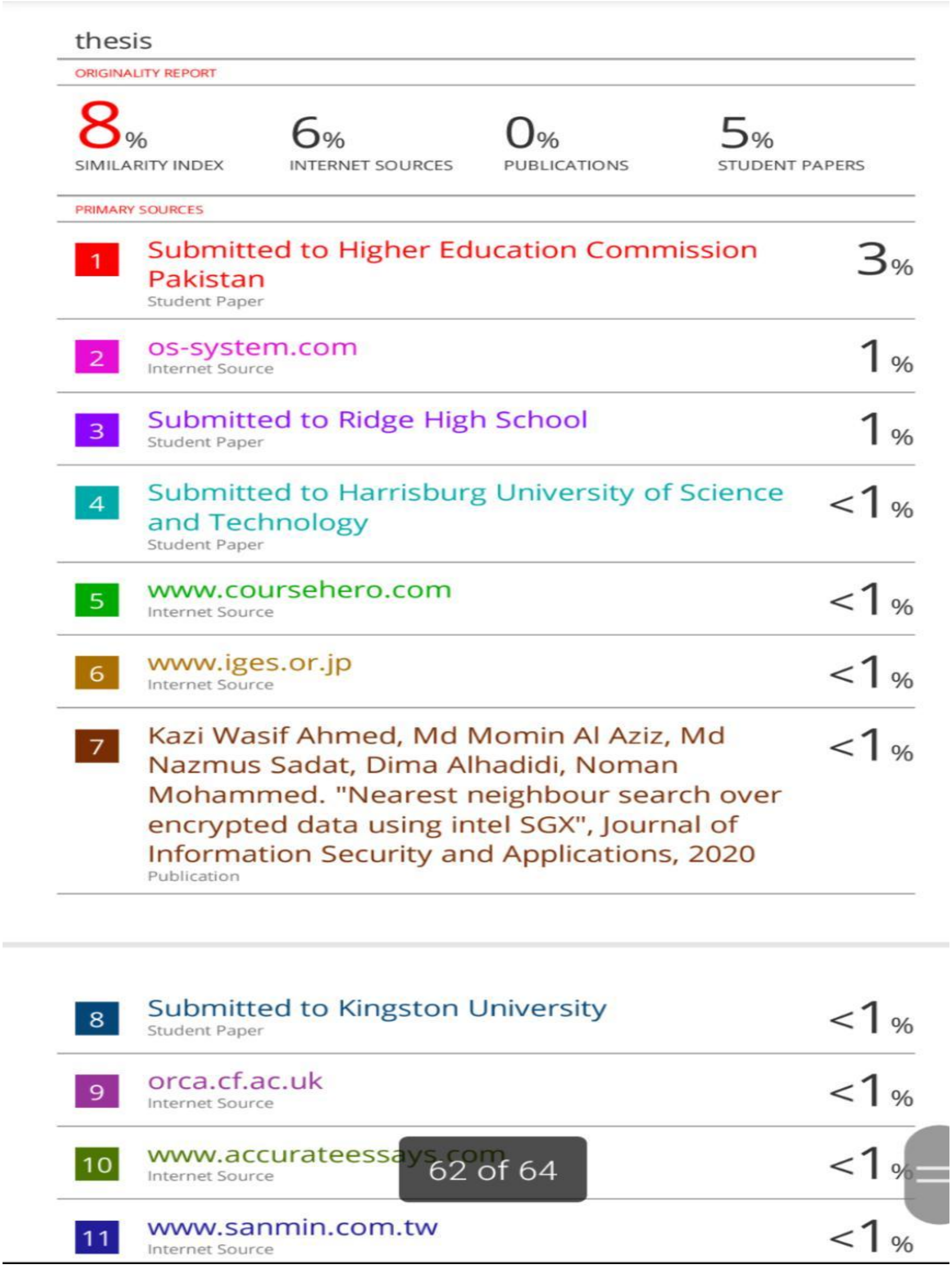
- Real-time – the actual time during which something takes place the computer may partly analyze the data in real time.

- User Interface – point of human-computer interaction and communication in a device i.e. screens, keyboards, etc.

- QT – a cross platform software for creating GUI.

6.1.2 Acronyms & Abbreviations

- C2 – Command and Control
- RAT – Remote Access Tools
- RAS– Remote Administrative Software
- SDGs – Sustainable Development Goals



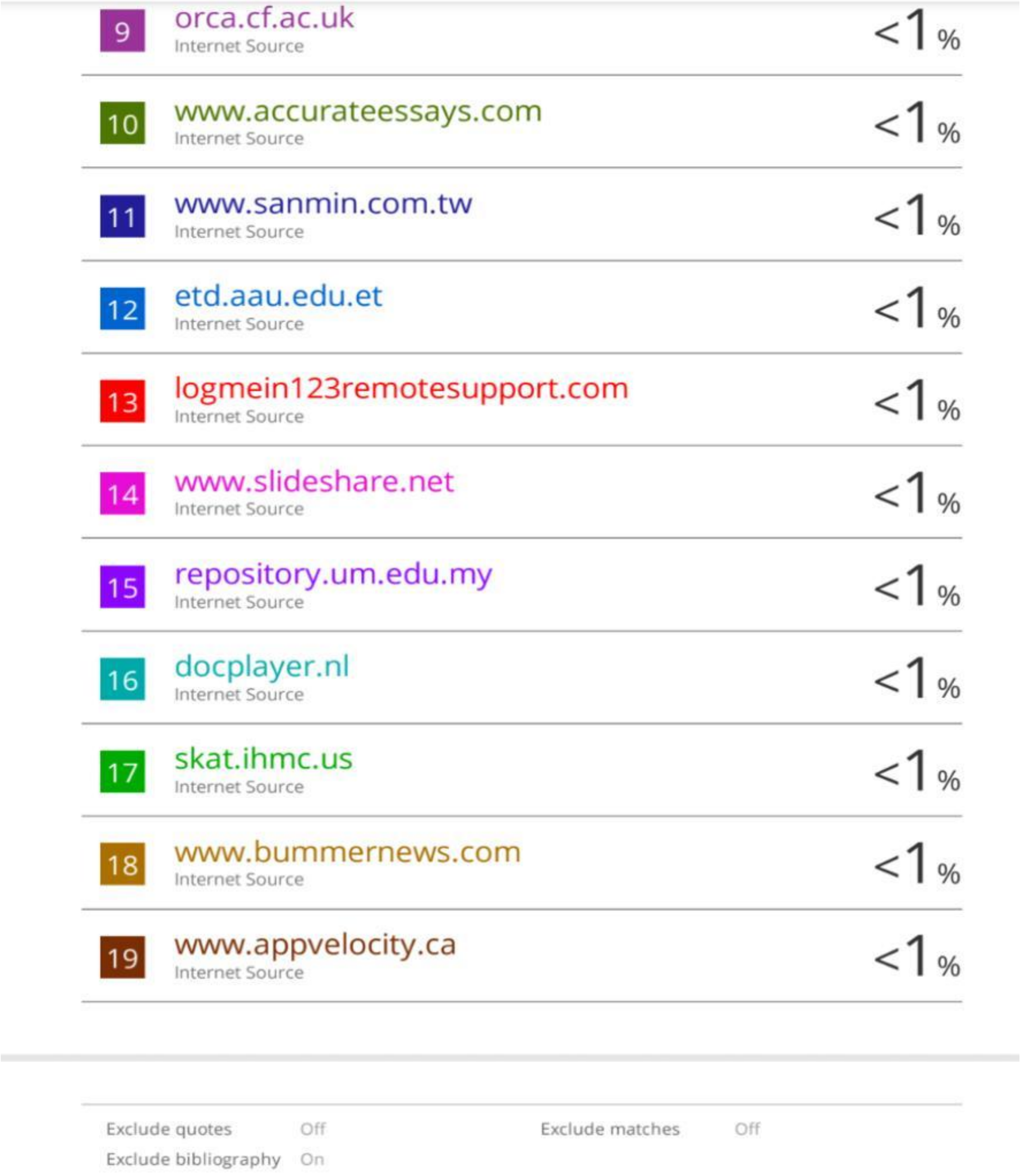
thesis

ORIGINALITY REPORT

8%	6%	0%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Higher Education Commission Pakistan Student Paper	3%
2	os-system.com Internet Source	1%
3	Submitted to Ridge High School Student Paper	1%
4	Submitted to Harrisburg University of Science and Technology Student Paper	<1%
5	www.coursehero.com Internet Source	<1%
6	www.iges.or.jp Internet Source	<1%
7	Kazi Wasif Ahmed, Md Momin Al Aziz, Md Nazmus Sadat, Dima Alhadidi, Noman Mohammed. "Nearest neighbour search over encrypted data using intel SGX", Journal of Information Security and Applications, 2020 Publication	<1%
8	Submitted to Kingston University Student Paper	<1%
9	orca.cf.ac.uk Internet Source	<1%
10	www.accurateessays.com Internet Source	<1%
11	www.sanmin.com.tw Internet Source	<1%



9	orca.cf.ac.uk Internet Source	<1 %
10	www.accurateessays.com Internet Source	<1 %
11	www.sanmin.com.tw Internet Source	<1 %
12	etd.aau.edu.et Internet Source	<1 %
13	logmein123remotesupport.com Internet Source	<1 %
14	www.slideshare.net Internet Source	<1 %
15	repository.um.edu.my Internet Source	<1 %
16	docplayer.nl Internet Source	<1 %
17	skat.ihmc.us Internet Source	<1 %
18	www.bummernews.com Internet Source	<1 %
19	www.appvelocity.ca Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		